Unit I

COURSE TITLE Building Design for Homeland Security

TIME 90 minutes

UNIT TITLE Introduction and Course Overview

OBJECTIVES

1. Describe the goal, objectives, and agenda for the course
2. Describe and find material in the course reference manual and student activity handout

SCOPE

The following topics will be covered in this unit:

1. Welcome and Opening Remarks
2. Instructor Introductions
3. Administrative Information
4. Student Introductions
5. Course Overview
6. Course Materials
7. Activity: Become familiar with Case Study materials

REFERENCES

1. Course Agenda
2. Course Goal and Objectives
3. EMI Evaluation Forms
4. FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*
5. Student Manual, Unit I
6. Case Study, Hazardville Information Company (HIC), for student activities
7. Unit I visuals

REQUIREMENTS

1. FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings* (one per student)
2. Instructor Guide
3. Student Manual (one per student)
4. Overhead projector or computer display unit
5. Unit I visuals
6. Chart paper, easel, and markers

UNIT I OUTLINE

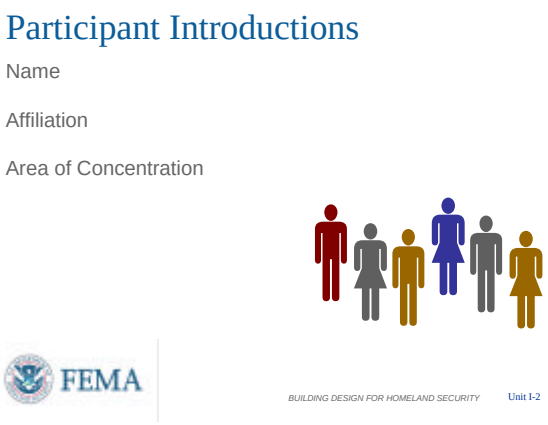
PREPARING TO TEACH THIS UNIT

- **Tailoring Content to the Local Area:** Review the Instructor Notes to identify topics that should focus on the local area. Plan how you will use the generic content, and prepare for a locally oriented discussion.

- **Optional Activity:** There are no optional activities in this unit.

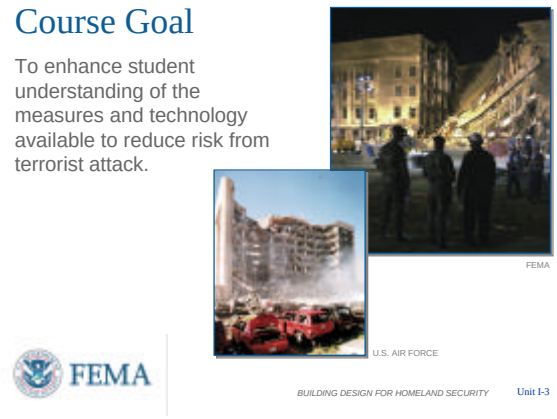
- **Activity:** The students will begin the familiarization with the Case Study materials. The Case Study is a complete risk assessment and analysis of mitigation options and strategies for a typical commercial office building located in a mixed urban-suburban environment business park. The assessment will use the DoD Antiterrorism standards and the GSA Interagency Security Criteria to determine Levels of Protection and identify specific vulnerabilities. Mitigation options and strategies will use the concepts provided in FEMA 426 and other standard reference materials such as the RS Means Building Security: Strategy and Costs, NFPA 5000, and other FEMA publications related to emergency planning and disaster recovery.

- Refer students to their Student Manuals for worksheets and activities.

INSTRUCTOR NOTES	CONTENT/ACTIVITY
VISUAL I-1	**Welcome and Opening Remarks**
	Welcome the students to the Building Design for Homeland Security Course. Introduce yourself, using: • Your name • A brief statement of background and experience Make the necessary administrative announcements, including: • Housing, parking, and meals • Attendance, start/stop times, breaks • Restroom locations • Messages and emergencies • Fire exits
VISUAL I-2	**Student Introductions**
	Ask the students to introduce themselves, including: • Name • Affiliation, brief background and experience statement, including work in the course topic area if applicable • One reason they are attending the course • What they plan to do with what they learn

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL I-3



Course Goal

The goal of this course is to enhance student understanding of the measures and technology available to reduce risk from terrorist attack.

Included in this understanding is the process for assessing risk to focus upon which mitigation measures have the greatest applicability and benefit. The students will understand the design approaches to mitigate manmade hazards and comprehend the trade-offs needed to optimize various design requirements.

VISUAL I-4

Course Objectives

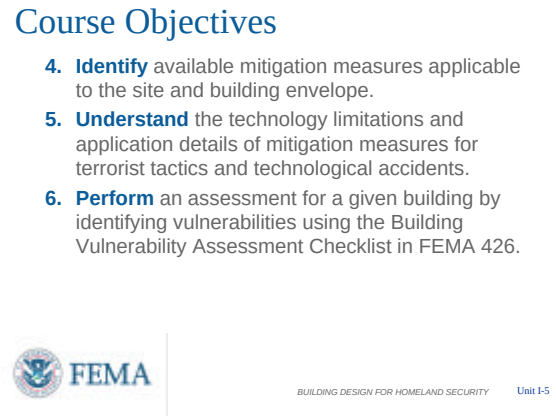
The primary target audience for this course will be engineers, architects, and state and local government and building officials with engineering and architectural backgrounds involved in mitigation planning and design to protect people and property against manmade hazards.

After attending the Building Design for Homeland Security course, participants should be able to:

1. Explain the basic components of the assessment methodology – threat/hazard, asset value, vulnerability, and risk, as applied to site, layout, and building.

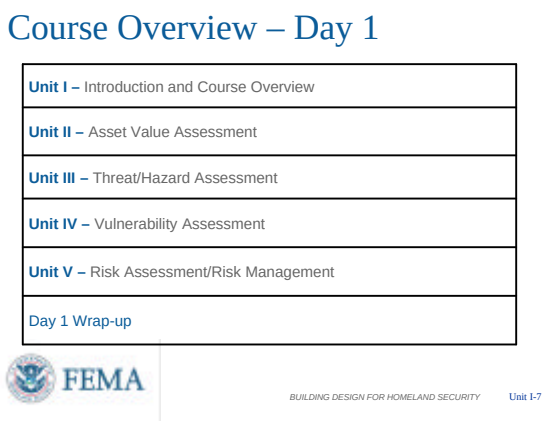
2. Understand the different assessment methodology approaches being used by Federal agencies and comprehend which approach to use for a given organizational structure.

3. Perform an assessment for a given building by identifying the assessment

INSTRUCTOR NOTES	CONTENT/ACTIVITY
	components and prioritizing the asset – threat/hazard pairs by their relative risk to focus resources upon mitigation measures that reduce risk.
VISUAL I-5	**Course Objectives**
	4. Identify available mitigation measures either in-place or for new design and comprehend their applicability to a given situation. 5. Understand the technology limitations and application details of mitigation measures for terrorist tactics and technological accidents involving explosive blast and agent release (chemical, biological, and radiological) to achieve a desired level of protection. 6. Use the **Building Vulnerability Assessment Checklist in FEMA 426** and adjust the assessment relative risk based upon the identified vulnerabilities.
VISUAL I-6	**Course Objectives**
	7. Select applicable mitigation measures and prioritize them based upon the final assessment relative risk values and associated estimated risk reduction provided so as to focus limited resources, all for a given situation. 8. Demonstrate that designing to mitigate building vulnerabilities against terrorist attacks has conflicts with other design requirements, resulting in trade-offs to achieve acceptable compliance and levels of performance among the differing regulations, codes, programs, operational requirements, and owner desires within the resources available.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL I-7



Course Overview

This course is a full 3 days in length and includes 11 units of instruction. Most instruction blocks have an associated student activity using a Case Study to emphasize the concepts taught and apply what was just learned.

A detailed schedule is located in your Student Manuals. This is Unit I – Introduction and Course Overview. It will review the other blocks of instruction and the course materials.

For the rest of the first day, the course will introduce the components of risk and how to determine risk. Unit II – Asset Value Assessment will discuss how to identify assets – or things to be protected, and how to assign a relative value to them.

Unit III will examine the Threat/Hazard Assessment process and identify the threats and hazards that could impact a building or site, review a Department of Defense methodology for defining threats, describe how threats and hazards may interact to increase damage, and providing numerical rating for the threat or hazard.

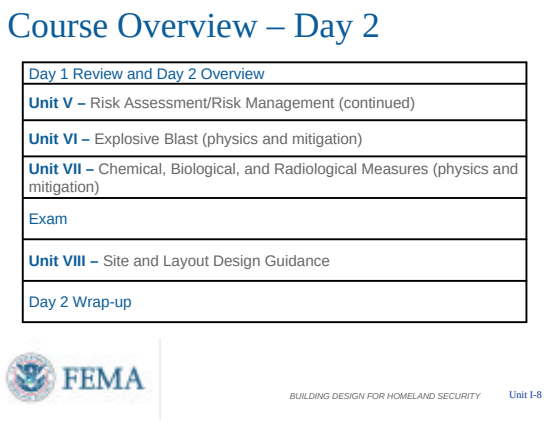
Unit IV will cover a Vulnerability Assessment, including what constitutes vulnerability and how to identify vulnerabilities using the Building Vulnerability Assessment Checklist.

Finally, the last Topic that will be covered on Day 1 is Unit V – Risk Assessment/Risk Management. Students will be taught what constitutes risk and how to determine a numerical value for risk and be introduced to the concept of the Design Basis Threat. This Unit will be completed on Day 2.

INSTRUCTOR NOTES

CONTENT/ACTIVITY

VISUAL I-8



At the end of each day, a short wrap-up session will be conducted to review the day's key concepts and provide an opportunity for students to ask any remaining questions.

Course Overview – Day 2

Day 2 will start with a quick review of Day 1 and then an overview of Day 2. Then Unit V will be completed.

At the completion of Unit V, students should have a firm grasp of risk and its components. They should know how to calculate a numeric value of risk based on its three components – asset value, threat rating, and vulnerability rating.

Units VI and VII will provide students with an understanding of some of the weapons commonly used by terrorists. Unit VI will cover explosive blast and Unit VII will cover chemical, biological, and radiological or CBR weapons.

No course would be complete without an exam – so there will be an open book short answer exam on Day 2. (Optional for VA Tech course.)

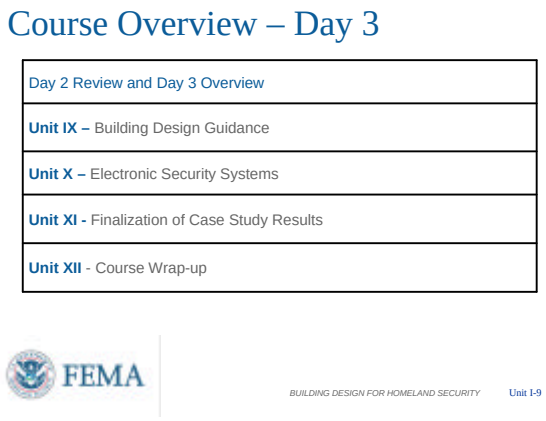
After the exam, the course will begin to explore mitigation options for reducing the risk and impact of terrorist attacks against buildings.

Unit VIII – Site and Layout Design Guidance will cover things you can do to mitigate terrorist attacks for the site – meaning from the property line up to the building.

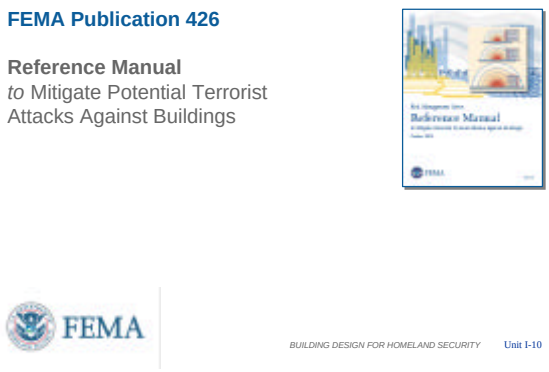
At the conclusion of Day 2, there will be another wrap-up session.

INSTRUCTOR NOTES

VISUAL I-9



VISUAL I-10



Confirm that each student has a copy of these materials.

CONTENT/ACTIVITY

Unit IX will explore mitigation options for the building envelope.

Unit X will introduce the basic concepts of electronic security systems.

As mentioned earlier – each block of instruction has an associated student activity using a Case Study to emphasize the concepts taught and apply what was just learned. In Unit XI, students will present the results of their work on the Case Study – highlighting their top three risks identified by the group, the vulnerabilities identified for these risks, and the top three mitigation measures to reduce vulnerability and risk.

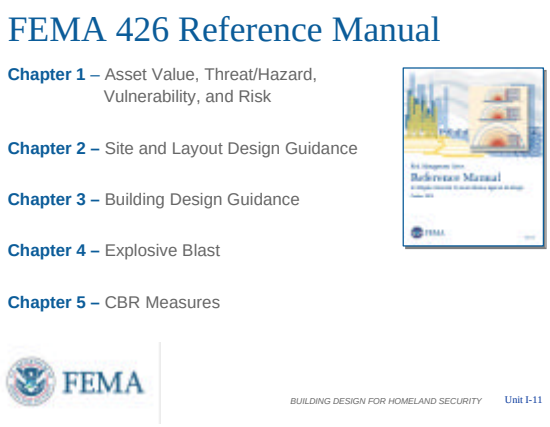
Finally, Unit XI will summarize the key points from the course and answer any final questions.

Course Materials

FEMA Publication 426, Reference CD, Student Manual

INSTRUCTOR NOTES

VISUAL I-11



As you begin the following walk-through of FEMA 426:

- Point out that the students will be following FEMA 426 throughout the course and will use some sections heavily during exercises. The course visuals include FEMA 426 page references for easy reference.

- Encourage them to flag key pages and passages with the provided Post-It® notes and highlighting.

Ask them to open FEMA 426 and follow along as you preview the contents.

CONTENT/ACTIVITY

FEMA 426 Reference Manual

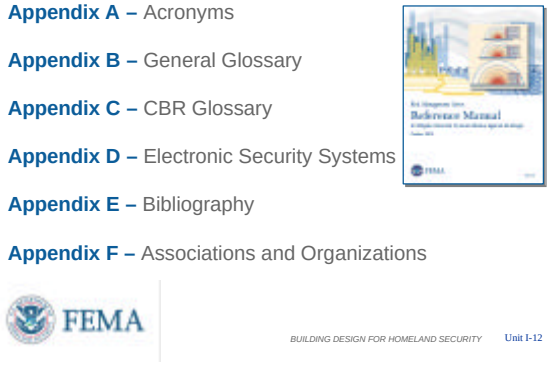
There are five chapters in the manual as listed here. This manual contains many how-to aspects based upon current information contained in FEMA, Department of Commerce, Department of Defense (including Army, Navy, and Air Force), Department of Justice, General Services Administration, Department of Veterans Affairs, Centers for Disease Control and Prevention/National Institute for Occupational Safety and Health, and other publications. It is intended to provide an understanding of the current methodologies for assessing asset value threat/hazard, vulnerability, and risk, and the design considerations needed to improve protection of new and existing buildings and the people occupying them. As needed, this manual should be supplemented with more extensive technical resources, as well as the use of experts when necessary.

Key concepts:

- Design Basis Threat
- Level of Protection
- Layers of Defense

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL I-12

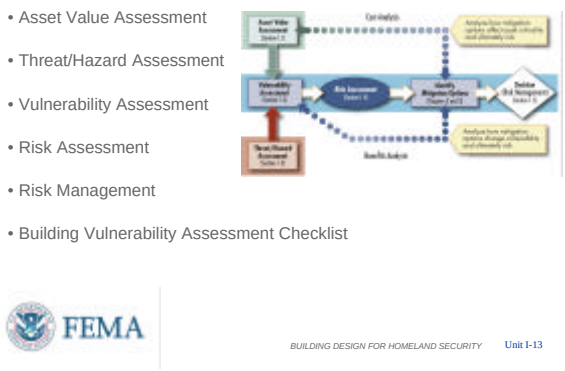


FEMA 426 Appendices

The manual also has six appendices to facilitate its use as a reference:

- Appendix A – Acronyms
- Appendix B – General Glossary
- Appendix C – CBR Glossary
- Appendix D – Electronic Security Systems
- Appendix E – Bibliography
- Appendix F – Associations and Organizations

VISUAL I-13



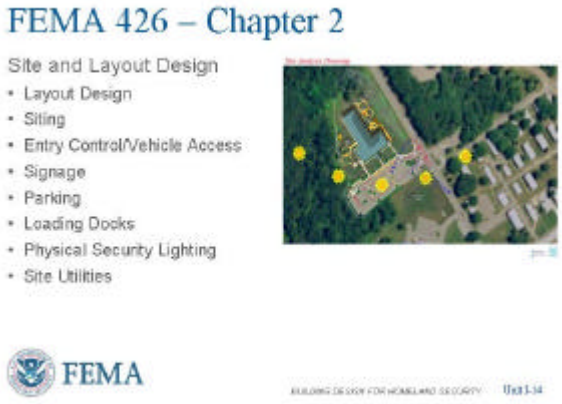
FEMA 426 - Chapter 1: Asset Value, Threat/ Hazard, Vulnerability, and Risk

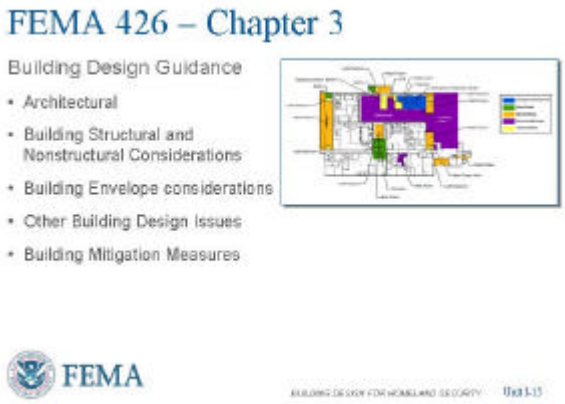
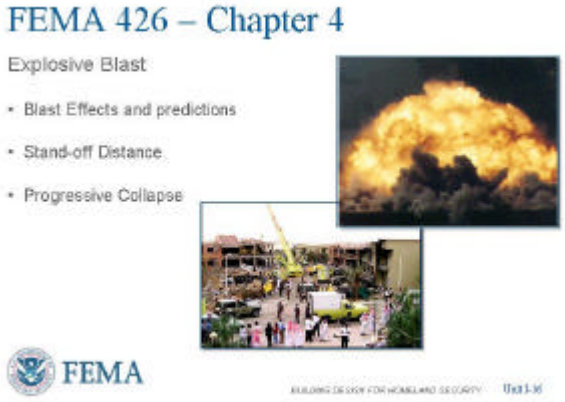
Chapter 1 presents selected methodologies to integrate threat/hazard, asset criticality, and vulnerability assessment information using applications such as the FEMA HAZUS-MH Geographic Information System (GIS) application to overlay imagery and maps to show access points, blast stand-off, and other site and building information.

The chapter also presents a risk matrix for the preparation of risk assessments. The topic areas of Chapter 1 are:

- Asset Value Assessment
- Threat/Hazard Assessment
- Vulnerability Assessment
- Risk Assessment
- Risk Management
- Building Vulnerability Assessment Checklist

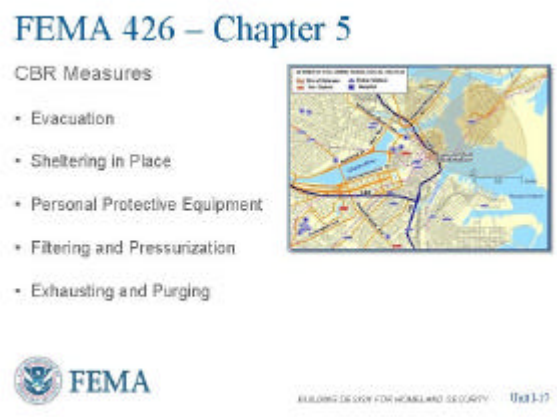
Finally, Chapter 1 provides an assessment checklist that compiles many best practices (based upon current technologies and scientific research) to consider during the

INSTRUCTOR NOTES	CONTENT/ACTIVITY
	design of a new building or renovation of an existing building.
	Assessment Flow Chart
	The assessment flow chart illustrates the process you will follow in conducting the assessment.
VISUAL I-14	**FEMA 426 - Chapter 2: Site Layout and Design Guidance**
	Chapter 2 discusses architectural and engineering design considerations (mitigation measures), starting at the perimeter of the property line, and includes the orientation of the building on the site. Therefore, this chapter covers issues outside the building envelope. Chapter 2 also discusses the following site layout and design topics: • Layout Design • Siting • Entry Control/Vehicle Access • Signage • Parking • Loading Docks • Physical Security Lighting • Site Utilities

INSTRUCTOR NOTES	CONTENT/ACTIVITY
VISUAL I-15	**FEMA 426 - Chapter 3: Building Design Guidance**
	Chapter 3 provides the same considerations for the building – its envelope, systems, and interior layout. The topic areas in Chapter 3 include: • Architectural • Building Structural and Nonstructural Considerations • Building Envelope Considerations • Other Building Design Issues • Building Mitigation Measures
VISUAL I-16	**FEMA 426 - Chapter 4: Explosive Blast**
	Chapter 4 provides a discussion of blast theory to understand the dynamics of the blast pressure wave, the response of building components, and a consistent approach to define levels of protection. Some of the details you will address include: • Building Damage • Blast Effects and Predictions • Stand-off Distance • Progressive Collapse

INSTRUCTOR NOTES

VISUAL I-17



CONTENT/ACTIVITY

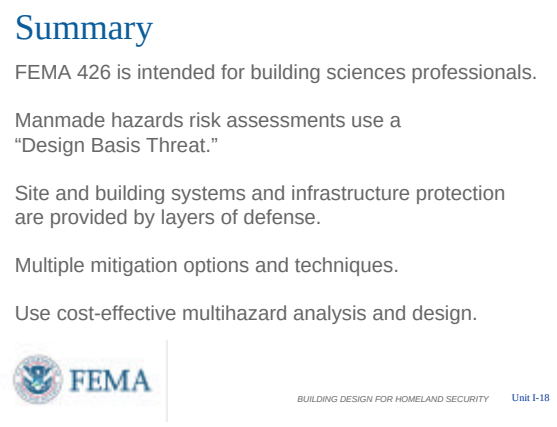
FEMA 426 - Chapter 5: CBR Measures

Chapter 5 presents chemical, biological, and radiological measures that can be taken to mitigate vulnerabilities and reduce associated risks for these terrorist tactics.

The concepts you should be familiar with at the end of the instruction include:

- Evacuation
- Sheltering in Place
- Personal Protective Equipment
- Filtering and Pressurization
- Exhausting and Purging

VISUAL I-18



Summary

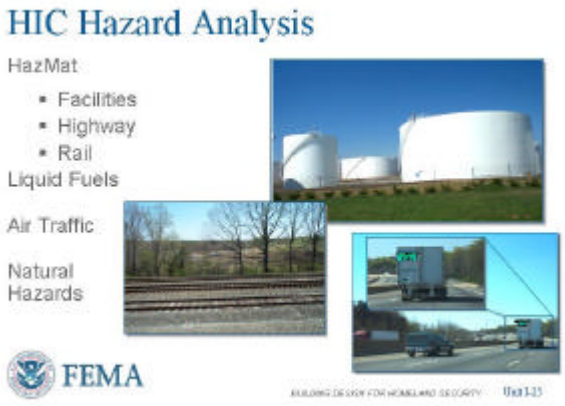
- FEMA 426 is intended for building sciences professionals.
- Manmade hazards risk assessments use a "Design Basis Threat" and "Levels of Protection" for manmade disaster and loads versus building codes for natural disaster and loads.
- Site and building systems and infrastructure protection are provided by layers of defense.
- Multiple mitigation options and techniques to deter, detect, deny, and devalue.
- Use cost-effective multi-hazard analysis and design.

INSTRUCTOR NOTES	CONTENT/ACTIVITY
VISUAL I-19 Case Study Activities In small group settings, apply concepts introduced in the course. Become conversant with contents and organization of FEMA 426.  FEMA BUILDING DESIGN FOR HOMELAND SECURITY Unit I-19	**Case Study Activities** Through case studies in small group settings, students will become conversant with the contents and organization of FEMA 426. • In small group settings, apply concepts introduced in the course • Become conversant with contents and organization of FEMA 426
VISUAL I-20 Unit I Case Study Activity **Hazardville Information Company Case Study Overview** **Requirements** Briefly review HIC case study materials. As a group, complete the worksheet. Use only the case study data to answer worksheet questions. FEMA BUILDING DESIGN FOR HOMELAND SECURITY Unit I-20	**Unit Case Study Activity** **Requirements** • Briefly review HIC Case Study materials (Appendix A of the Student Manual) • As a group, complete the worksheet • Use only the Case Study data to answer worksheet questions
VISUAL I-21 HAZARDVILLE INFORMATION COMPANY (HIC) **Case Study** FEMA BUILDING DESIGN FOR HOMELAND SECURITY Unit I-21	**Introduction to the Case Study** The Case Study activities throughout this course provide opportunities, in a small group setting, to apply concepts introduced in each unit. These activities will enable participants to become conversant with FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*. Participants will be able to use the document readily during the process of mitigating

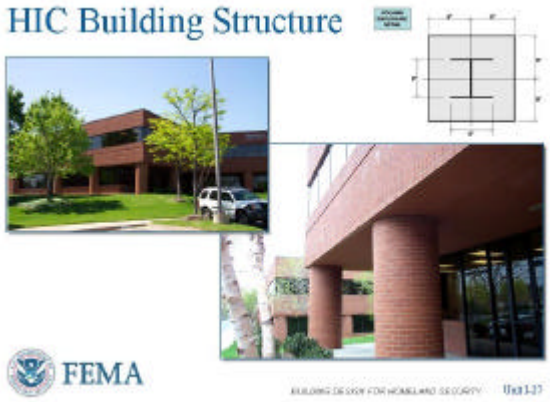
INSTRUCTOR NOTES	CONTENT/ACTIVITY
Divide participants into small groups of five to seven. Participants should work in these groups for the remainder of the small group sessions. Refer participants to the Unit I Case Study activity in the Student Manual. Members of the instructor staff should be available to answer questions and assist groups as needed. At the end of 20 minutes, reconvene the class and facilitate group reporting.	potential damage from terrorist attacks against buildings. The activities are designed to "walk" participants through the same assessment and design steps using a Case Study involving a hypothetical building and associated data about the threat environment. **Hazardville Information Company (HIC)** The Hazardville Information Company (HIC) is a fictional entity created for this course (see Appendix A of the Student Manual). • It is a composite of actual sites and buildings with actual systems typical of a number of commercial buildings. The Case Study mainly addresses threat information related to manmade hazards: • Explosive blast • Chemical, biological, and radiological agents • Armed attack • Cyber attack Each section of the Case Study activity includes: • Examination of specific aspects of the Case Study data. • Assessment of data and application to the Case Study of concepts and processes addressed in the unit. • Completion of worksheets that demonstrate participant mastery of unit learning objectives.

INSTRUCTOR NOTES	CONTENT/ACTIVITY
	General Requirements Each participant is responsible for completion of his or her own worksheets. In addition, the small groups will produce a completed worksheet for each unit's activity and post it in a designated location. Group members are encouraged to discuss activity requirements and collaborate on completion of the worksheets. To facilitate this process, select a leader and a recorder.
VISUAL I-22  	**Hazardville Information Company** **Activity Requirements** • Turn to Appendix A, the Case Study materials in the Student Manual and briefly peruse the document. • Read the "familiarization" questions on the following worksheet and, as a group, complete the worksheet. • Use only the Case Study data to answer worksheet questions. Take 20 minutes to complete this activity. Solutions will be reviewed in the plenary group.

INSTRUCTOR NOTES	CONTENT/ACTIVITY
VISUAL I-23	**Hazardville Information Company** The Hazardville Information Company supports approximately 1,000 users and 100 applications as a primary data center and as a disaster recovery backup site. HIC has over 130 employees and approximately 80-100 employees are in the building at any given time
VISUAL I-24	**Threats/Hazards** • Terrorism • Intelligence • Crime Note the site location, terrain, parking, and other commercial buildings around HIC.
VISUAL I-25	**Threats/Hazards** • HazMat • Natural Hazards Note the major interstate and rail lines near HIC.

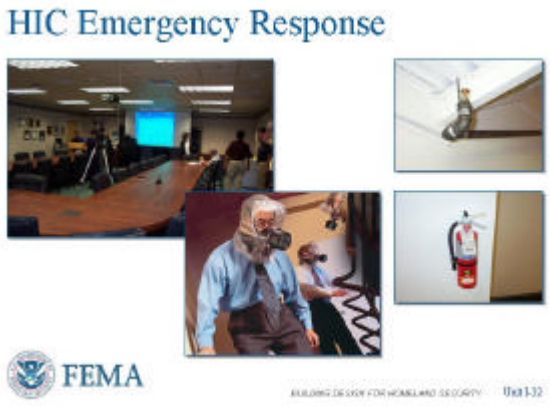


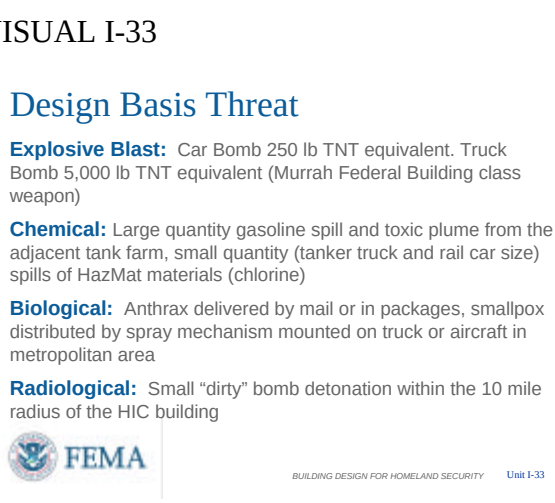
INSTRUCTOR NOTES	CONTENT/ACTIVITY
VISUAL I-26	**HIC Building Data** • Structural • Mechanical • Electrical • IT • Physical Security Note the parking lot, building entry and exit access points, loading docks, building functions, and building infrastructure.
VISUAL I-27	**HIC Building Structure** The Case Study will review the building structure and envelope to identify vulnerabilities and mitigation options. Note the percentage of glass on the exterior walls, overhangs, and type of construction.
VISUAL I-28	**HIC Mechanical Systems** The Case Study will review mechanical systems, plumbing, and piping to identify vulnerabilities and mitigation options. Note the exposed meters and ground level air intake.



INSTRUCTOR NOTES	CONTENT/ACTIVITY
VISUAL I-29	**HIC Electrical Systems** The Case Study will review primary electrical utilities and backup power to identify vulnerabilities and mitigation options. Note the exposed electrical transformers, critical utility entry points, and redundancies.
VISUAL I-30	**HIC Physical Security** The Case Study will review physical security systems, equipment, and procedures to identify vulnerabilities and mitigation options. Note the locations of sensors, lights, access points, and type of badges or card readers.
VISUAL I-31	**HIC IT Systems** The Case Study will review key IT systems to include the data center and communications to identify vulnerabilities and mitigation options. Note the type of flooring, penetrations, mixed cable and fiber, racks.

INSTRUCTOR NOTES	CONTENT/ACTIVITY
VISUAL I-32	**HIC Emergency Response** Determine the location, availability, and readiness condition of emergency response assets, and the state of training of building staff in their use. Note the location and type of protective equipment, safe haven or shelter in place options, and mass notification capability.
VISUAL I-33	**Design Basis Threat** • Explosive Blast • Chemical • Biological • Radiological ("dirty" bomb)
VISUAL I-34	**Design Basis Threat** • Criminal Activity/Armed Attack • Cyber Attack

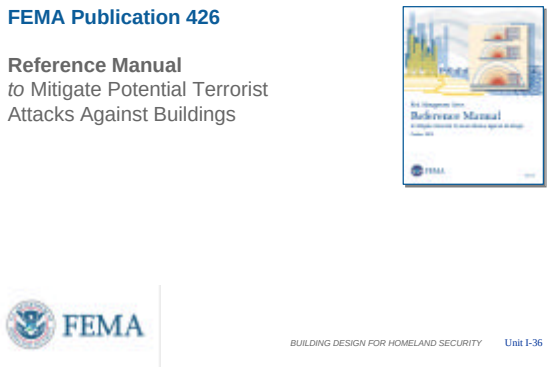




INSTRUCTOR NOTES

VISUAL I-35

VISUAL I-36



Exam Questions #A18 and B17

CONTENT/ACTIVITY

Level of Protection and Layers of Defense

The Case Study will use both the GSA and DoD Levels of Protection to evaluate vulnerabilities against and to develop mitigation options.

A key design strategy and concept is "Layers of Defense". The elements of a layered system are:

- Deter
- Detect
- Deny
- Devalue

Summary

The objective of this course is to provide a comprehensive approach to reducing the physical damage to structural and non-structural components of buildings and related infrastructure, focusing on six specific types of facilities:

- Commercial office facilities
- Retail commercial facilities
- Light industrial and manufacturing
- Health care
- Local schools
- Higher education

Most importantly, the course provide participants with a solid foundation on:

- Design Basis Threat
- Levels of Protection
- Layers of Defense

INSTRUCTOR NOTES	CONTENT/ACTIVITY

Transition

In this course, you will learn how to perform a multi-hazard risk assessment of a building and become familiar with the key concepts of to protect buildings from manmade threats and hazards:

- Asset Value
- Design Basis Threat
- Level of Protection
- Layers of Defense
- Vulnerability Assessment
- Risk Assessment
- Mitigation

Using the approach and guidance provided in FEMA 426, the majority of building owners should be able to complete a risk assessment of their building in a few days and identify the primary vulnerabilities, mitigation options, and make informed decisions on the ability of their building to survive, recover, and operate should an attack or event occur.

For the rest of the first day, the course will introduce the components of risk and how to determine risk.

- Unit II – Asset Value Assessment
- Unit III – Threat/Hazard Assessment
- Unit IV – Vulnerability Assessment
- Unit V – Risk Assessment/Risk Management

UNIT I CASE STUDY ACTIVITY:
HAZARDVILLE INFORMATION COMPANY (HIC)
CASE STUDY OVERVIEW

Requirements

Turn to the Appendix A Case Study materials in the Student Manual and briefly peruse the document. Read the "familiarization" questions on the following worksheet, and as a group, complete the worksheet. Use only the Case Study data to answer worksheet questions. Information has been limited in an effort to focus the activity.

Question	Answer	Page # in Case Study
1. What are the major transportation nodes in the surrounding area?	A major interstate highway is located within ¼ mile of the HIC Headquarters. CSX Transportation and Norfolk-Southern Railway maintain a transportation corridor about ½ mile from HIC. There appear to be no restrictions on the material carried along these rail lines. Two airports are in the vicinity of HIC. One is a major international airport approximately 8 miles away. The other is a small, but busy general aviation airport less than 2 miles away.	A-3, A-28 – A-30
2. What life safety assets are available, and what are their response times?	• Wet pipe sprinkler system • 20 hand-held dry chemical fire extinguishers • Firestation 2½ miles away. Seven others within 5 miles of the site. Response time: 8-10 minutes • Hospital ER 5 miles away	A-16, A-17, A-27
3. Who are the building's primary occupants and visitors?	• HIC has over 130 employees and approximately 80 to 100 employees are in the building at any given time • Fortune 500 companies • National and regional banks and credit unions • A major airline • Large prime defense contractors • Government agencies, including one classified client	A-1, A-2

4. What hazards may affect HIC?	• Hazardous materials • Liquid fuels • Air traffic • Natural disasters • Manmade disasters	A-5, A-6, A-28 – A-30
5. What are the prevalent weather/wind conditions at HIC?	The prevailing weather pattern for the area in the summer and fall is from the south Atlantic and the Gulf of Mexico. Warm, moist air brings thunderstorms and higher humidity. In the fall, cooler air from the north and west returns. Winter weather blasts across the state from the northern or central part of the continent. With no other weather activity, the prevailing wind is normally from the west-northwest.	A-6
6. What are the critical functions of HIC?	• Computer/data processing • Wired/wireless networking • Information Technology • Communications	A-21 – A-24
7. What are the components of HIC's critical utility infrastructure?	• Electrical systems • Mechanical systems • Gas supply • Communications systems • Emergency response systems	A-12 – A-19
8. What are the components of HIC's critical building infrastructure?	• Parking • Entryways • Exits • Loading docks	A-11, A-12, A-16
9. What personnel are key to the operation of HIC?	HIC has over 130 employees and approximately 80 to 100 employees are in the building at any given time.	A-2

Unit II

COURSE TITLE Building Design for Homeland Security

TIME 75 minutes

UNIT TITLE Asset Value Assessment

OBJECTIVES

1. Identify the assets of a building or site that can be affected by a threat or hazard
2. Explain the components used to determine the value of an asset
3. Determine the critical assets of a building or site
4. Provide a numerical rating for the asset and justify the basis for the rating

SCOPE

The following topics will be covered in this unit:

1. The core functions and critical infrastructure listed on the threat-vulnerability matrix.
2. Various approaches to determine asset value – Federal Emergency Management Agency, Department of Defense, Department of Justice, and Veterans Affairs.
3. A rating scale and how to use it to determine an asset value.
4. Activity: Identify the assets to consider in the Case Study and determine the asset value for each asset of interest.

REFERENCES

1. FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings,* pages 1-10 to 1-14
2. Student Manual, Unit II
3. Case Study – Hazardville Information Company
4. Unit II visuals

REQUIREMENTS

1. FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Building*s (one per student)
2. Instructor Guide
3. Student Manual (one per student)
4. Overhead projector or computer display unit
5. Unit II visuals
6. Chart paper, easel, and markers

UNIT II OUTLINE

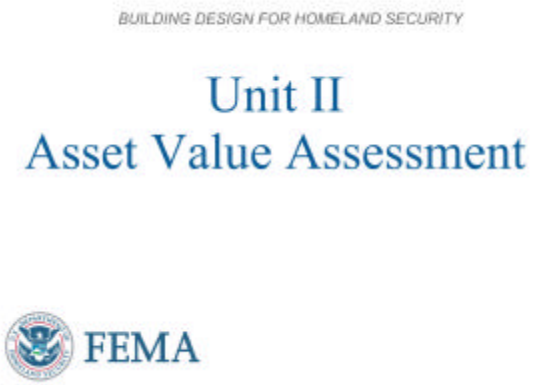
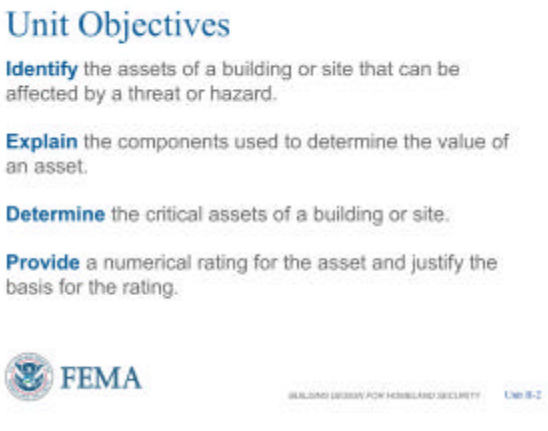
PREPARING TO TEACH THIS UNIT

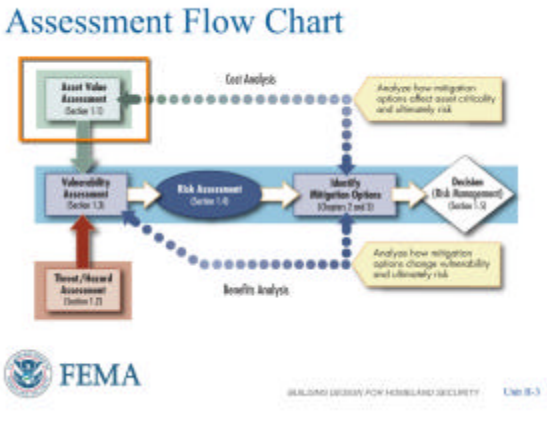
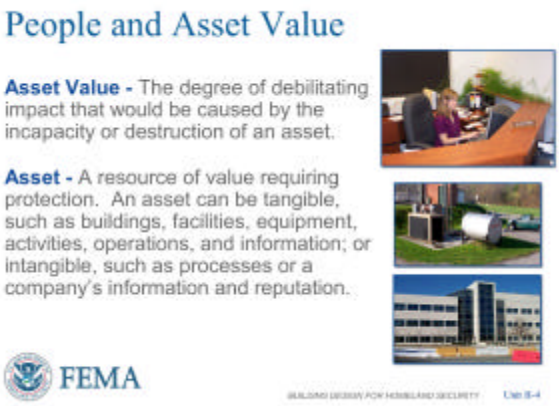
- **Tailoring Content to the Local Area:** Review the Instructor Notes to identify topics that should focus on the local area. Plan how you will use the generic content, and prepare for a locally oriented discussion.

- **Optional Activity:** There are no optional activities in this unit.

- **Activity:** The Instructor will discuss the generic core functions and critical infrastructure associated with the Case Study building as listed on the threat-vulnerability matrix. The Instructor will walk through the examples, describing the asset in relation to the Case Study and applying the asset value rating approach. The students will then apply these techniques (asset identification and asset value rating) to the Case Study to identify and rate the assets found in the Case Study. The students will have to quickly review/scan the mission statement, building data, building structure, mechanical systems, electrical systems, physical security, information systems, and communications to have a sense of the value of the asset to the Hazardville Information Company.

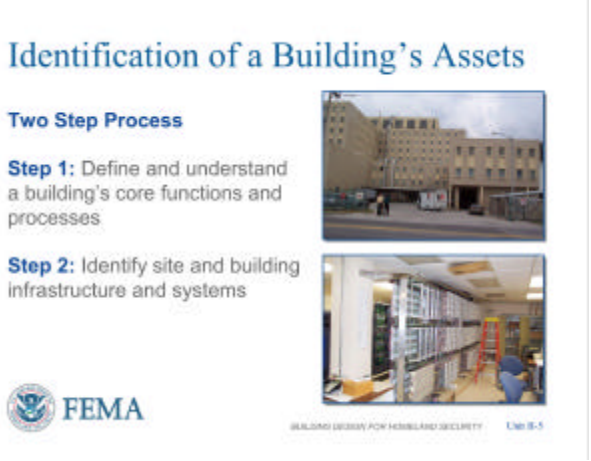
- Refer students to their Student Manuals for worksheets and activities.

INSTRUCTOR NOTES	CONTENT/ACTIVITY
VISUAL II-1  	**Introduction and Unit Overview** This is Unit II, Asset Value Assessment. This section will describe how to perform an asset value assessment (the first step in the assessment process), to identify people and asset values. Key to this process is interviewing stakeholders including owners, facility staff and tenants.
VISUAL II-2  	**Unit Objectives** At the end of this unit, the student should be able to: 1. Identify the assets of a building or site that can be affected by a threat or hazard. 2. Explain the components used to determine the value of an asset. 3. Determine the critical assets of a building or site. 4. Provide a numerical rating for the asset and justify the basis for the rating.

INSTRUCTOR NOTES	CONTENT/ACTIVITY
VISUAL II-3	**Assessment Flow Chart**
	Reviewing the Assessment Flow Chart, the first step in the risk assessment process is to determine asset value. An asset is anything you want to protect because of its value, its need to maintain business continuity, and/or its difficulty in replacing within a required timeline.
VISUAL II-4	**People and Asset Value**
	Understanding asset criticality is comparable to strategic planning in that the building owner should understand the mission of the organization, the resources that are used to perform that mission, how those resources interface with one another to achieve goals, and how the organization would cope or maintain business continuity if the asset(s) were lost. In general terms, asset value can be considered the economic replacement cost for infrastructure and equipment. People are a building's most critical asset.
Exam Questions #A1 and B2	

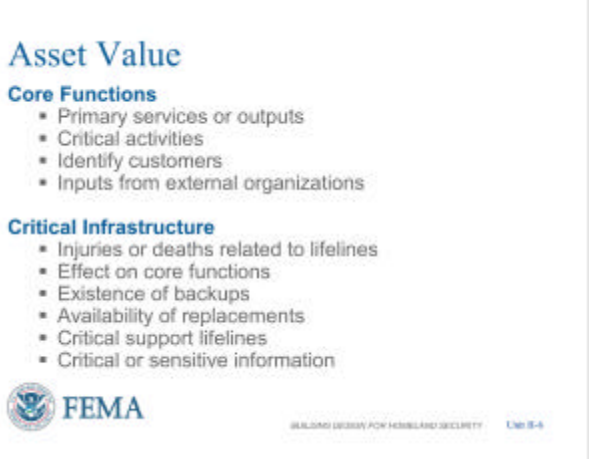
INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL II-5



Exam Questions #A2 and B1

VISUAL II-6



Identification of a Building's Assets

Identifying a building's critical assets is accomplished in a two-step process.

Step 1: Define and understand a building's core functions and processes.

Step 2: Identify site and building infrastructure and systems:

- Critical components/assets
- Critical information systems and data
- Life safety systems and safe haven areas
- Security areas

Asset Value

The objective in the initial step is to determine the core functions for the building that will enable it to continue to operate or provide services after an attack. This focuses the assessment team on the key areas of the building. Factors include:

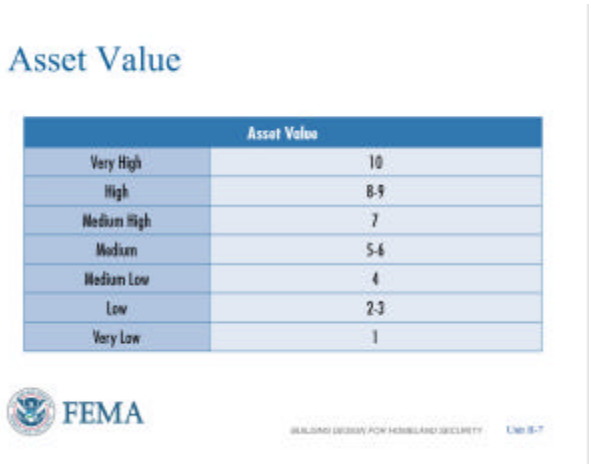
- What are the primary services?
- What critical activities take place at the building?
- Who are the building's occupants and visitors?

To help evaluate and rank critical infrastructure, consider the following factors:

- Injuries or deaths related to critical infrastructure damage
- Effect on core functions
- Existence of backups, systems redundancy
- Availability of replacements
- Critical support lifelines
- Critical or sensitive information

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL II-7



Quantifying Asset Value

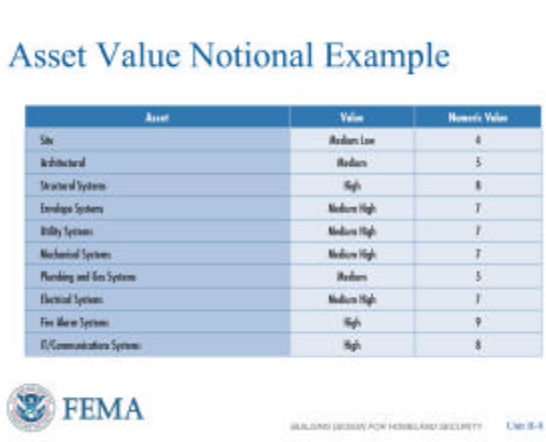
After a building's assets requiring protection has been identified, they are assigned a value. The asset value is the degree of debilitating impact that would be caused by the incapacity or destruction of the building's assets.

FEMA Publication 426 uses a combination of a seven-level linguistic scale and a ten-point numeric scale.

- **Very High** – Loss or damage of the asset would have exceptionally grave consequences, such as extensive loss of life, widespread severe injuries, or total loss of primary services, core processes, and functions.
- **High** - Loss or damage of the asset would have grave consequences, such as loss of life, severe injuries, and loss of primary services.
- **Medium High** – Loss or damage of the asset would have serious consequences, such as serious injuries, or impairment of core processes and functions for an extended period of time.
- **Medium** – Loss or damage of the asset would have moderate to serious consequences.
- **Medium Low** – Loss or damage of the asset would have moderate consequences, such as minor injuries, or minor impairment of core functions and processes.
- **Low** – Loss or damage of the asset would have minor consequences or impact.
- **Very Low** – Loss or damage of the asset would have negligible consequences or impact.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL II-8

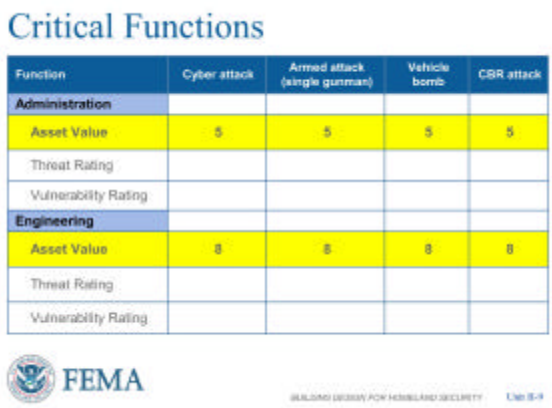


Asset Value Notional Example

The key assets for this a notional example by system are listed and an asset value rating is entered into the site critical functions matrix.

HVAC mechanical systems in most buildings will likely be medium high (7).

VISUAL II-9



Critical Functions Matrix

List functions down the left side and threats across the top.

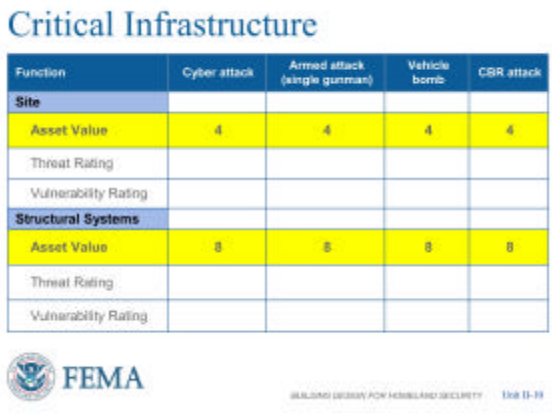
In general, the asset value for a given function is the same for all threats and the matrix helps to identify the primary functions in a quantitative form. The functions matrix is people oriented and is subjective, but the completed matrix should provide a guide to vulnerabilities and risks. An organization with few administrative staff but a large engineering group is used in this example.

Note the value is the same for all threat pairs to reflect the people and organization impact losses that could occur should the asset be lost.

Note: The Asset Value under the Administration and Engineering functions is highlighted. A medium value rating (5) is assigned for the Administrative function threat as they are a small part of the total organization. A medium Asset Value was assigned for the Engineering Function threat pairs. A high Asset Value rating (8) was assigned for the Engineering Function threat pairs as they account for over half of the organization.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL II-10



Note: The Asset Value rating under the Site and Structural Systems is highlighted. A medium low Asset Value rating (4) would be an initial value for the site infrastructure threat pairs because the site has a well defined and protected perimeter, but the site can be impacted by guns and bombs and economic replacement costs will be acceptable. A high Asset Value rating (8) would be an initial value for the Structural System threat pairs since it is multi-story and subject to progressive collapse and cannot be replaced.

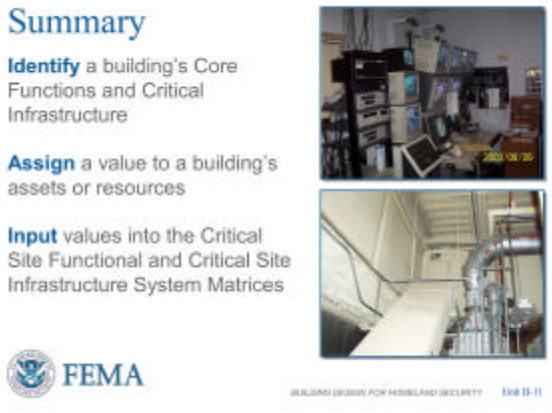
Critical Infrastructure Matrix

List Infrastructure down the left side and threats across the top.

In general, the asset value for a given infrastructure asset is the same for all threats and is usually the economic cost of replacement. The value can be changed to reflect intangibles such as duration of loss, loss of production capability, etc. For this example, a building is on a site with a controlled perimeter fence and adequate stand-off distance. The structure is multi-story and a single building houses all functions.

Note that the value is the same for all threat pairs to reflect the economic and organization impact losses that could occur over time should the asset be lost.

VISUAL II-11

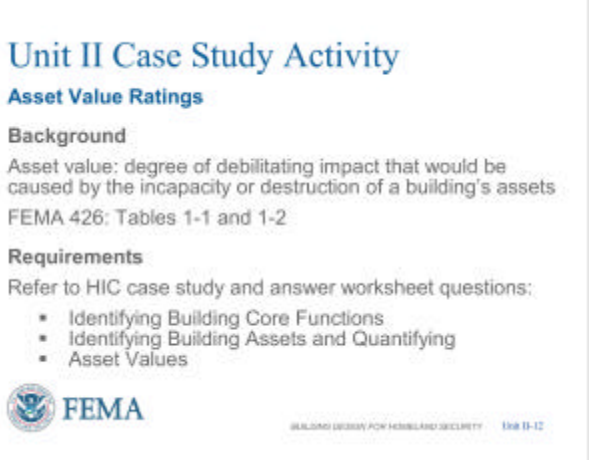


Summary

- Identify a building's Core Functions and Critical Infrastructure
- Assign a building's assets or resources a value
- Insert values into the Critical Site Functional matrix and the Critical Site Infrastructure System matrix

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL II-12



Refer participants to FEMA 426 and the Unit II Case Study activity in the Student Manual.

Members of the instructor staff should be available to answer questions and assist groups as needed.

At the end of 25 minutes, reconvene the class and facilitate group reporting. Keep in mind that there are no incorrect answers. It is more important to be able to clearly explain and support the underlying rationale for the values that have been assigned.

Student Activity

Asset value is the degree of debilitating impact that would be caused by the incapacity or destruction of a building's assets.

- **Page 1-13 of FEMA 426** provides an **Asset Value Scale (Table 1-1)** to quantify asset value, as well as definitions of the ratings.
- **Table 1-2 on page 1-14 of FEMA 426** provides a format to summarize the value of the major categories of a building's assets.

Activity Requirements

- Working in previously assigned small groups, refer to the HIC Case Study and answer the worksheet questions.

Take 25 minutes to complete this activity. Solutions will be reviewed in plenary group.

TRANSITION

Unit III will cover a Threat/Hazard Assessment and Unit IV will cover Vulnerability Assessment.

UNIT II CASE STUDY ACTIVITY: ASSET VALUE RATINGS

Asset value is the degree of debilitating impact that would be caused by the incapacity or destruction of a building's assets. **Page 1-13 of FEMA 426** provides an Asset Value Scale **(Table 1-1)** to quantify asset value, as well as definitions of the ratings. **Table 1-2 on page 1-14 of FEMA 426** provides a format to summarize the value of the major categories of a building's assets.

Requirements

Referring to the HIC Case Study, answer the following questions:

Identifying Building Core Functions

1. What are HIC's primary services or outputs?

   I T services support for private and government organizations. HIC supports over 1,000 users and over 100 applications to include field technicians and help desk.

2. What critical activities take place at HIC?

   Computer-based data processing, storage, and disaster recovery.

3. Who are the building's occupants and visitors?

   HIC employees and clients; business park neighbors are a mix of government and commercial organizations. Front parking area is unrestricted.

4. What inputs from external organizations are required for HIC's success?

   Utilities and communications supplies/vendors; hardware and software applications vendors; client data and support

Identifying Building Assets and Quantifying Asset Values

Refer to **Table 1-2 in FEMA 426** and use the descriptions of these asset categories in the HIC Case Study. Consider the questions on **page 1-11 in FEMA 426** and rate HIC's assets as:

- Very High (10)
- High (8-9)
- Medium High (7)
- Medium (5-6)
- Medium Low (4)
- Low (2-3)
- Very Low (1)

HIC Critical Functions Asset Rating

Asset	Value	Numeric Value	Rationale
1. Administrative	Medium Low	4	Redundancy and staff skills that can be replaced. Senior managers and financial systems in the same area make the function a key area to protect. Low to medium economic cost to replace.
2. Engineering/IT Technicians	Medium	5	Staff skills that can be replaced, but require specialized expertise. Key equipment and resources may not be replaceable. High economic cost to replace.
3. Loading Dock/Warehouse	Medium	5	Single point of entry into the interior and through which all major shipping and receiving occurs. Low to medium economic cost to replace.
4. Data Center	Very High	10	Primary function and organizational critical. Many key staff and critical equipment. Very high economic cost to replace.
5. Communications	High	8	Primary function and organizational critical. A few key staff and critical equipment. High economic cost to replace.
6. Security	Medium High	7	Access and monitoring systems, security records and location make the function critical to the organization. Key staff. Low to medium

			economic cost to replace.
7. Housekeeping	Very Low	1	Easily replaced, no critical skills or equipment.

HIC Critical Infrastructure Asset Rating

Asset	Value	Numeric Value	Rationale
1. Site	Medium	5	No defined perimeter that HIC can control or segregate. Open sight lines and straight line vehicle approaches. Building owner does not own the site on which the building is located, but the location is critical to access and support to clients.
2. Architectural	Medium	5	Signage and business office information couple the building to other park tenants (geographically clustered, centralized. $10 to $20 per square foot lease cost.
3. Structural Systems	Medium	5	Two-story building probably is not going to experience progressive collapse, but over 50 percent of exterior is glazing. $10 to $20 per square foot lease cost.
4. Envelope Systems	Medium	5	Fairly tight envelope, newer construction, CBR agents not likely to penetrate into interior through wall cracks or roof gaps without longer time.

5. Utility Systems	Medium	5	Well protected and buried, but single lines.
6. Mechanical Systems	Medium High	7	Single HVAC system supports multiple HVAC AHUs and interior spaces. High economic cost to replace. Loss of business revenue.
7. Plumbing and Gas Systems	Medium	5	Wet pipe sprinkler system only means of fire protection.
8. Electrical Systems	Medium High	7	Single-point vulnerability and organizational critical. High economic cost to replace. Loss of business revenue.
9. Fire Alarm Systems	Medium	5	Wet pipe sprinkler system only means of fire protection.
10. IT/Communications Systems	Very High	10	Single-point vulnerability and organizational critical. High economic cost to replace. Loss of business revenue.

Unit III

COURSE TITLE Building Design for Homeland Security

TIME 75 minutes

UNIT TITLE Threat/Hazard Assessment

OBJECTIVES

1. Identify the threats and hazards that may impact a building or site
2. Define each threat and hazard using the Department of Defense methodology
3. Provide a numerical rating for the threat or hazard and justify the basis for the rating
4. Define the Design Basis Threat and Levels of Protection

SCOPE

The following topics will be covered in this unit:

1. From what offices is threat and hazard information available.
2. The spectrum of event profiles for terrorism and technological hazards from FEMA 386-7.
3. The five components used by DoD to define a threat and how it can be applied to the Homeland Security Advisory System.
4. Various approaches to determine threat rating – Federal Emergency Management Agency, Department of Defense, Department of Justice, and Veterans Affairs.
5. A rating scale and how to use it to determine a threat rating.
6. Activity: Identify the threats and hazards to consider in the Case Study. As an absolute minimum, consider explosive blast and agents (chemical, biological, and radiological). Determine the threat rating for the minimum threat/hazards.

REFERENCES

1. FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*, pages 1-1 to 1-18
2. Student Manual, Unit III
3. Case Study – Hazardville Information Company
4. Unit III visuals

REQUIREMENTS

1. FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings* (one per student)
2. Instructor Guide

3. Student Manual (one per student)
4. Overhead projector or computer display unit
5. Unit III visuals
6. Chart paper, easel, and markers

UNIT III OUTLINE

PREPARING TO TEACH THIS UNIT

- **Tailoring Content to the Local Area:** Review the Instructor Notes to identify topics that should focus on the local area. Plan how you will use the generic content, and prepare for a locally oriented discussion.

  The Instructor will begin this unit with a brief discussion of terrorism and technological hazards worldwide and within the United States. The probability of natural hazards and how they are considered during design will be compared to the probability of manmade hazards, both terrorism and technological accidents. This sets the stage for identifying where to get information about threats and hazards.

  Next, the Instructor will use FEMA 386-7 to describe the spectrum of tactics or events that can occur. This leads into the five components used to define a threat (or hazard) and one interpretation of the Homeland Security Advisory System.

  Various threat and vulnerability rating systems will be discussed to understand the different methodologies and their applicability to different situations. A simplified threat rating approach will be presented that can be used during a design charette for new construction or major renovation. This FEMA 426 approach forms the basis of the Unit III student activity.

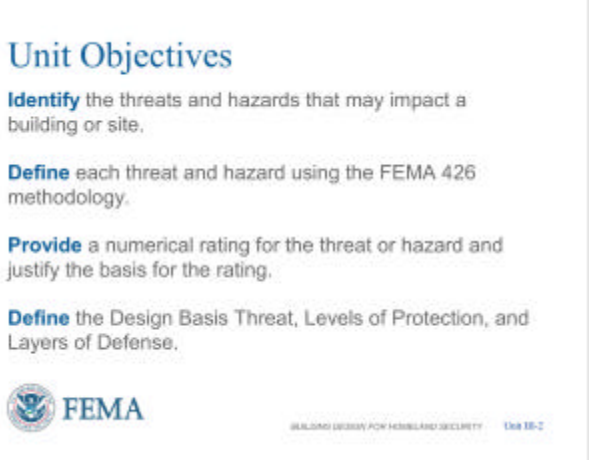
- **Optional Activity:** There are no optional activities in this unit.

- **Activity:** The Instructor will use one threat/hazard example from the Case Study to focus students on the student activity. The Instructor will walk through the example, describing the threat and the threat rating approach.

  The students will then apply these techniques (threat identification, threat description, and threat rating) to the Case Study to identify and rate the threat from explosive blast and agents (chemical, biological, and radiological). Note that these event profiles can result from terrorism or technological hazards.

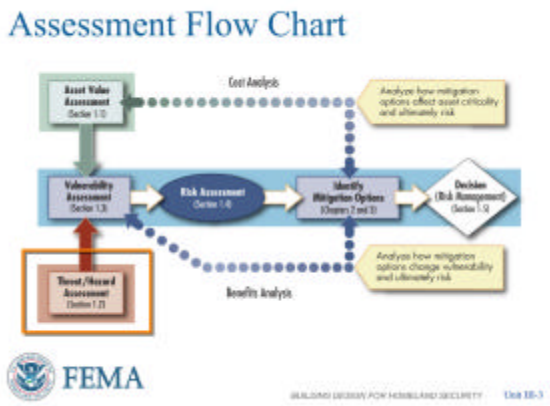
  Remind the students that they were exposed to the Case Study during the Unit I Introduction and Course Overview. They will have to read the Threat Analysis and Hazard Analysis portions that will cover primarily explosive blast and agents, rather than looking at all potential threats/hazards within the timeframe available. A review of the GIS portfolio will also be recommended for gaining threat and hazard information.

- Refer students to their Student Manuals for worksheets and activities.

INSTRUCTOR NOTES	CONTENT/ACTIVITY
VISUAL III-1  The students will apply these techniques (threat identification, threat description, and threat rating) to the Case Study to identify and rate the threat from explosive blast and agents (chemical, biological, and radiological). Note that these event profiles can result from terrorism or technological hazards.	**Introduction and Unit Overview** This is Unit III Threat Hazard Assessment. The unit starts with a brief discussion of terrorism and technological hazards worldwide and within the United States. The probability of natural hazards and how they are considered during design will be compared to the probability of manmade hazards, both terrorism and technological accidents. The five components used to define a threat (or hazard) and one interpretation of the Homeland Security Advisory System are used to illustrate how assessment analysis can be coupled with increasing threat levels.
VISUAL III-2  	**Unit Objectives** At the end of this unit, you should be able to: 1. Identify the threats and hazards that may impact a building or site. 2. Define each threat and hazard using the FEMA 426 methodology. 3. Provide a numerical rating for the threat or hazard and justify the basis for the rating. 4. Define the Design Basis Threat, Levels of Protection, and Layers of Defense.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

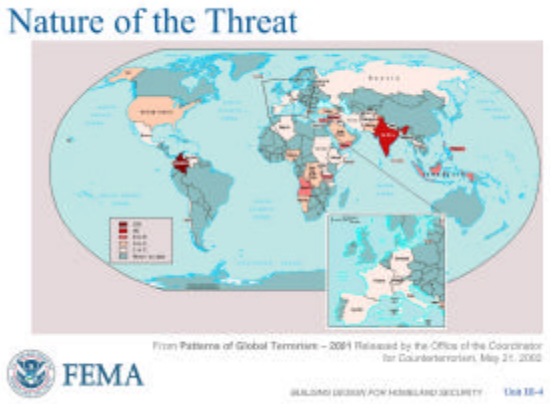
VISUAL III-3



Assessment Flow Chart

Reviewing the Assessment Flow Chart, the Threat Assessment is the next step in the risk assessment process.

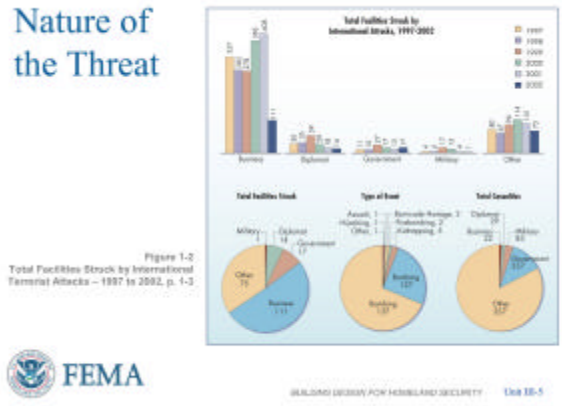
VISUAL III- 4



Nature of the Threat

With enhanced migration of terrorist groups from conflict-ridden countries, the formation of extensive international terrorist infrastructures and the increased reach of terrorist groups, terrorism has become a global concern.

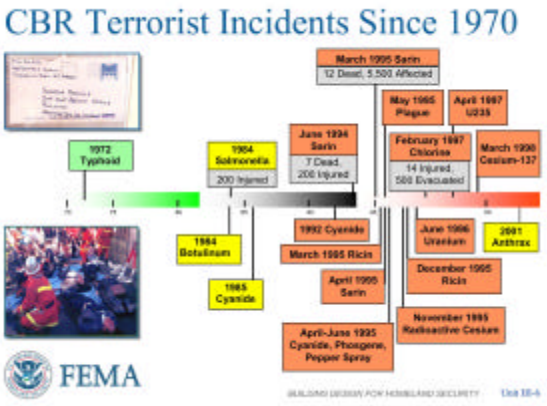
VISUAL III- 5



Nature of the Threat

Terrorism and physical attacks on buildings have continued to increase in the past decade. The geographical isolation of the United States is not a sufficient barrier to prevent an attack on U.S. cities and citizens. These data from the Department of State *Patterns of Global Terrorism 2002* demonstrate the far reaching incidents and diverse natures and targets of recent terrorist attacks.

INSTRUCTOR NOTES	CONTENT/ACTIVITY
VISUAL III-6	**CBR Terrorist Incidents Since 1970**



CBR attacks have been used since ancient times and, in the past 20 years, over 50 attacks have occurred. CBR attacks require the right weather, population, and dispersion to be effective. Recent attacks have had limited effectiveness or have been conducted on a relatively small scale. Future attacks with Weapons of Mass Destruction could occur on a regional or global scale.

VISUAL III-7

Hazard

- **Hazard -** A source of potential danger or adverse condition.
- **Natural Hazards** are naturally-occurring events such as floods, earthquakes, tornadoes, tsunami, coastal storms, landslides, hurricanes, and wildfires. A natural event is a hazard when it has the potential to harm people or property. (FEMA 386-2, *Understanding Your Risks*). The risks of natural hazards may be increased or decreased as a result of human activity.

VISUAL III-8

Threat/Manmade Hazard

- **Technological Accidents** are incidents that can arise from human activities such as manufacturing, transportation, storage, and use of hazardous materials. For the sake of simplicity, it is assumed that technological emergencies are accidental and that their consequences are unintended.
- **Terrorism** is the unlawful use of force and violence against persons or property to intimidate or coerce a government, the

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

civilian population, or any segment thereof, in furtherance of political or social objectives. (28 CFR, Section 0.85)

VISUAL III-9

Identify Each Threat/Hazard

- **Table 1-3 in FEMA 426 (page 1-17)** outlines the broad spectrum of terrorist threats and technological hazards. Some of the items are listed here.

- While we can think of terrorist tactics and technological hazards (such as HazMat releases), a runaway truck crashing into a power line, a storage tank, or a telephone pedestal can be equally detrimental. Similarly, surveillance of a company's operations may divulge company trade secrets that are detrimental to the economic bottom line.

VISUAL III-10

Define Each Threat/Hazard

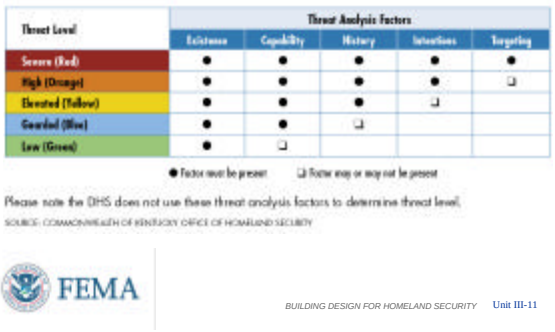
Part of the understanding of each hazard or threat is to walk through these five threat analysis factors as laid out by the Department of Homeland Security to define the threat in regard to the aggressors or perpetrators that may want to cause harm.

First, what groups or organizations exist/are known? Do they have capability among themselves or is that capability readily obtainable locally? Do they have a history of terrorist acts and what are their tactics? What are the intentions of the aggressors against the government, commercial enterprises, industrial sectors, or individuals? Finally, has it been determined that targeting (planning a tactic or seeking vulnerabilities) is actually occurring or being discussed?

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

For technological hazards, these same questions take a different perspective. Does anything that can be a hazard (or be attacked causing collateral damage) exist within a given distance of the building in question?

VISUAL III-11



Determine Threat Level for Each Hazard

Applying the factors to make terrorist threat predictions is shown here. As each factor (existence, capability, history, intention, and targeting) is confirmed, the potential threat increases.

It shows how the threat analysis factors information about one or more terrorist groups as interpreted by the local intelligence community can be used to determine a threat level. However, some people may prefer the simple High, Medium, and Low ratings.

VISUAL III-12

Threat Sources

A manmade threat/hazard analysis requires coordination with security and intelligence organizations that understand the locality, the region, and the Nation. These organizations include the police department (whose jurisdiction includes the building or site), the local state police office, and the local office of the FBI. In many areas of the country, there are threat coordinating committees, including FBI Joint Terrorism Task Forces, that facilitate the sharing of information.

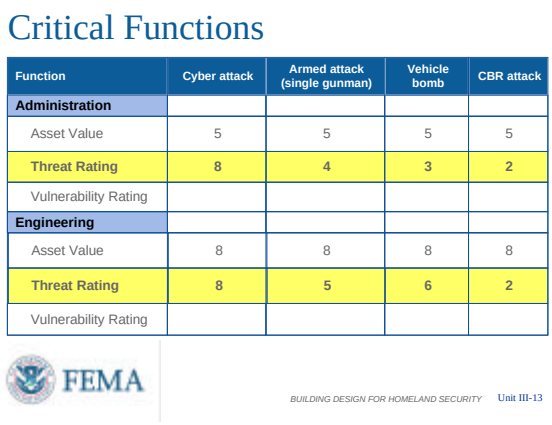
Exam Questions #A3 and B4

Note: For technological hazards, it is also important to gather information from the local fire department and hazardous materials (HazMat) unit, Local Emergency Planning Committee (LEPC), and State Emergency Response Commission (SERC). LEPC and

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

SERC are local and state organizations established under a U.S. Environmental Protection Agency (EPA) program. They identify critical facilities in vulnerable zones and generate emergency management plans. Additionally, most fire departments understand which industries in the local area handle the most combustible materials and the HazMat unit understands who handles materials that could have a negative impact upon people and the environment. In many jurisdictions, the HazMat unit is part of the fire department.

VISUAL III-13



Note: The Threat Rating values for the Administration and Engineering functions are highlighted. The ratings run from low to high for each threat pair that are derived from the site-specific threat analysis and the values shown are to illustrate a typical analysis.

Critical Functions

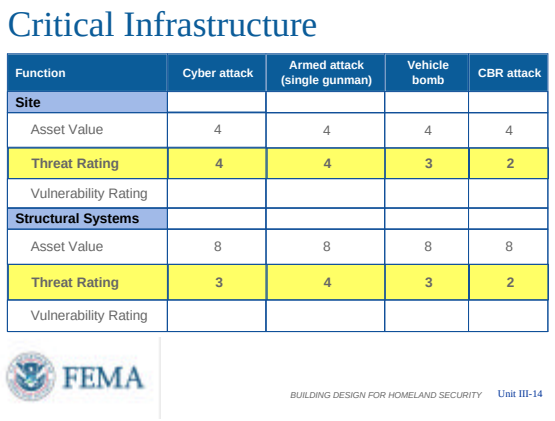
After each threat/hazard has been identified and defined, the threat level for each threat/hazard must be defined. The threat rating is a subjective judgment of a terrorist threat based on existence, capability, history, intentions, and targeting.

It is a snapshot in time, and can be influenced by many factors, but the given threat value will typically be the same for each function (going down the columns). Organizations that are dispersed in a campus environment may have variation.

On a scale of 1 to 10, 1 is a very low probability and 10 is a very high probability of a terrorist attack.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL III-14



Critical Infrastructure

The site Critical Infrastructure matrix lists Infrastructure down the left side and threats across the top.

The threat rating under the Structural Systems is highlighted. A medium threat rating (3) was assigned under cyber attack, armed attack (4), and vehicle bomb (3); and a low threat rating was assigned under CBR attack (2).

VISUAL III-15

Design Basis Threat

Having applied a systems engineering evaluation process to determine a building's critical functions, infrastructure, and having an understanding of the aggressors' likely weapons and attack delivery mode, the next step in the process of quantifying a building's risk assessment is determining the "Design Basis Threat."

After review of the preliminary information bout the building functions, infrastructure and threats, senior management should establish the "Design Basis Threat" and select the desired "Level of Protection".

Note: Facility designers need to have the size and type of bomb, vehicle, gun, CBR, or other threat tactics, weapons, or tools identified in order to provide an appropriate level of protection.

There are several methodologies and assessment techniques that can be used. Historically, the U.S. military methodology (with a focus on explosive effects, CBR, and personnel protection) has been used extensively for military installations and other national infrastructure assets.

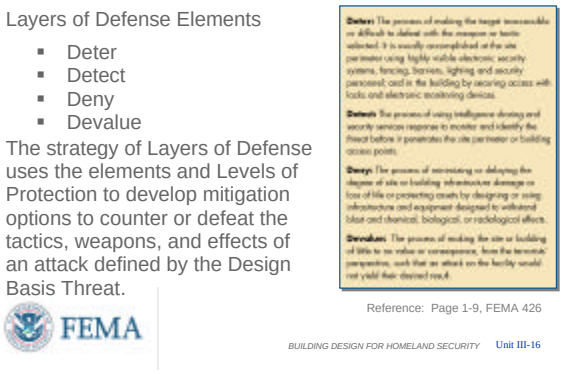
INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

- The Department of State (DOS) adopted or co-developed many of the same blast and CBR design criteria as DoD and GSA.
- The GSA further developed criteria for federal buildings as a result of the attack on the Murrah Federal Building.
- The Department of Commerce (DOC) Critical Infrastructure Assurance Office (CIAO) established an assessment framework, which focused on information technology infrastructure.

VISUAL III-16

Levels of Protection

Layers of Defense elements
- Deter
- Detect
- Deny
- Devalue

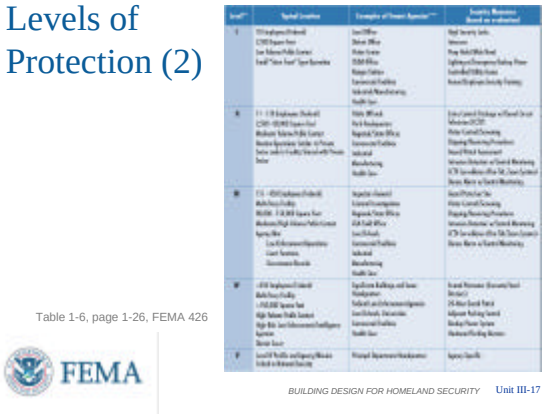


Exam Questions #A17 and B18

VISUAL III-17

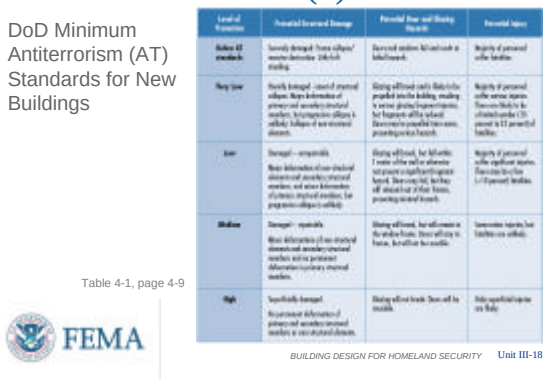
Levels of Protection

This table – extracted from the U.S. Department of Justice's *Vulnerability Assessment of Federal Facilities* (1995) – presents a series of security measures for typical sizes and types of sites, in addition to a transferable example of appropriate security measures for typical locations and occupancies.



INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

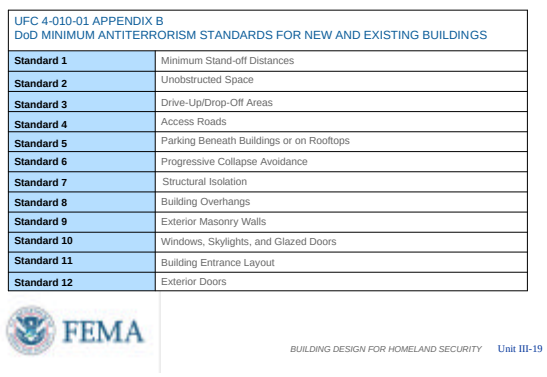
VISUAL III-18



DoD Minimum Antiterrorism (AT) Standards for New Buildings

In contrast to the GSA security levels and criteria, the DoD correlates levels of protection with potential damage and expected injuries.

VISUAL III-19



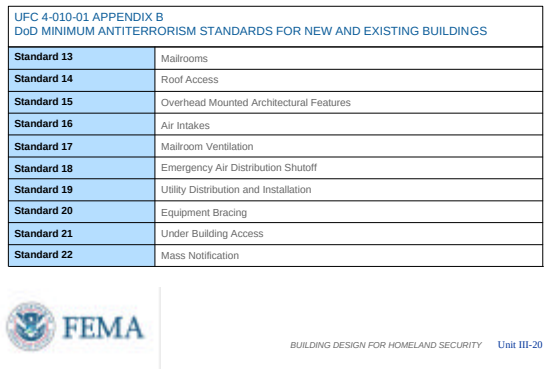
Levels of Protection

DoD Antiterrorism Standards 1-12.

Highlight Standards 1, 2, and 4, and refer to the Building Vulnerability Assessment Checklist questions for blast evaluation.

Each standard has text for each Level of Protection that describes the Design Basis Threat and mitigation options or recommendations.

VISUAL III-20



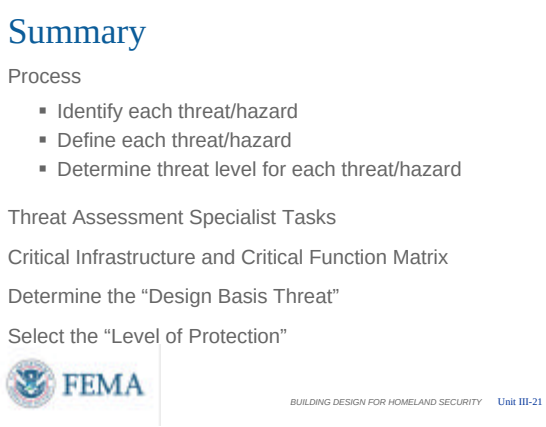
Levels of Protection

DoD Antiterrorism Standards 13 – 22.

Highlight Standards 17, 18, and 19, and impacts on HVAC.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL III-21



Summary

The process for developing threat assessments:

- Identify each threat/hazard
- Define each threat/hazard
- Determine threat level for each threat/hazard

Use Federal, state, or local law enforcement to help determine threat ratings.

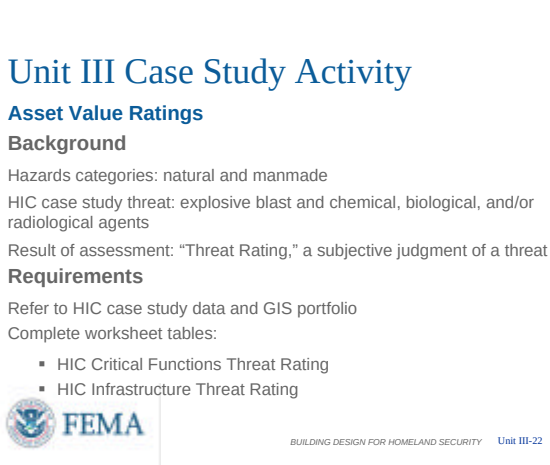
Complete the Critical Infrastructure and Critical Function Matrices.

Establish the Design Basis Threat.

Select the Level of Protection (using DoD standards).

Use Layers of Defense strategy to mitigate attack and develop mitigation options.

VISUAL III-22



Student Activity

After assets that need to be protected are determined, an assessment is performed to identify the threats and hazards that could cause harm to the building and the inhabitants of the building.

Hazards are categorized into two groups:

- Natural
- Manmade

While natural hazards could logically be expected to affect the HIC, the Case Study describes the threat from:

- Explosive blast
- Chemical, biological, and/or radiological "agents"

Refer participants to FEMA 426 and the Unit III Case Study activity in the Student Manual.

INSTRUCTOR NOTES	CONTENT/ACTIVITY
Members of the instructor staff should be available to answer questions and assist groups as needed. At the end of 20 minutes, reconvene the class and facilitate group reporting.	• Cyber attack • Armed attack The result of this assessment is a "Threat Rating." The threat rating is a subjective judgment of a threat based on: • Existence • Capability • History • Intentions • Targeting The rating scale is a scale of 1 to 10: • 1 is a very low probability of a terrorist attack • 10 a very high probability. **Activity Requirements** Working in small groups, refer to the HIC Case Study and GIS portfolio, and complete the worksheet tables for: • HIC Critical Functions • HIC Infrastructure Take 20 minutes to complete this activity. Solutions will be reviewed in plenary group. **Transition** Unit IV will cover a Vulnerability Assessment and Unit V will cover Risk Assessment/Risk Management.

UNIT III CASE STUDY ACTIVITY: THREAT/HAZARD RATING

After assets that need to be protected are determined, an assessment is performed to identify the threats and hazards that could cause harm to the building and the inhabitants of the building. Hazards are categorized into two groups: natural and manmade. While natural hazards could logically be expected to affect the HIC, the Case Study only describes the threat from explosive blast and from chemical, biological, and/or radiological "agents."

The result of this assessment is a "Threat Rating." The threat rating is a subjective judgment of a threat based on existence, capability, history, intentions, and targeting. The rating scale is a scale of 1 to 10, with 1 a very low probability of a terrorist attack and 10 a very high probability.

Requirements

Refer to the HIC Case Study data and GIS portfolio and complete the following worksheets. Each student will interpret the HIC threat information and should have a number close to the value shown. Any function with key IT systems connected to the Internet should get high cyber values. Functions that are susceptible to blast should get high numbers. A CBR attack will impact the entire facility.

HIC Critical Functions Threat Rating

Function	Cyber Attack	Armed Attack	Vehicle Bomb	CBR Attack	Rationale
1. Administration	6	3	6	4	Local and international groups with the capability, intentions, and targeting expertise are known to be in the area.
2. Engineering/IT Technicians	5	3	6	4	Local and international groups with the capability, intentions, and targeting expertise are known to be in the area.

3. Loading Dock/ Warehousing	5	3	6	4	Local and international groups with the capability, intentions, and targeting expertise are known to be in the area.
4. Data Center	9	3	6	4	Local and international groups with the capability, intentions, and targeting expertise are known to be in the area.
5. Communications	5	3	6	4	Local and international groups with the capability, intentions, and targeting expertise are known to be in the area.
6. Security	5	3	6	4	Local and international groups with the capability, intentions, and targeting expertise are known to be in the area.
7. Housekeeping	2	3	6	4	Local and international groups with the capability, intentions, and targeting expertise are known to be in the area.

HIC Infrastructure Threat Rating

Function	Cyber Attack	Armed Attack	Vehicle Bomb	CBR Attack	Rationale
1. Site	1	3	6	4	Local and international groups with the capability, intentions, and targeting expertise are known to be in the area.
2. Architectural	1	3	6	4	Local and international groups with the capability, intentions, and targeting expertise are known to be in the area.
3. Structural	1	3	6	4	Local and international groups with the capability, intentions, and targeting expertise are known to be in the area.
4. Envelope Systems	1	3	6	4	Local and international groups with the capability, intentions, and targeting expertise are known to be in the area.

5. Utility Systems	3	5	6	4	Local and international groups with the capability, intentions, and targeting expertise are known to be in the area.
6. Mechanical Systems	3	5	6	4	Local and international groups with the capability, intentions, and targeting expertise are known to be in the area.
7. Plumbing and Gas Systems	2	3	6	4	Local and international groups with the capability, intentions, and targeting expertise are known to be in the area.
8. Electrical Systems	3	3	6	4	Local and international groups with the capability, intentions, and targeting expertise are known to be in the area.
9. Fire Alarm Systems	2	3	6	4	Local and international groups with the capability, intentions,

					and targeting expertise are known to be in the area.
10. IT/ Communications Systems	10	3	6	4	Local and international groups with the capability, intentions, and targeting expertise are known to be in the area.

Unit IV

COURSE TITLE Building Design for Homeland Security

TIME 105 minutes

UNIT TITLE Vulnerability Assessment

OBJECTIVES

1. Explain what constitutes a vulnerability
2. Identify vulnerabilities using the Building Vulnerability Assessment Checklist
3. Understand that an identified vulnerability may indicate that an asset is vulnerable to more than one threat or hazard and that mitigation measures may reduce vulnerability to one or more threats or hazards
4. Provide a numerical rating for the vulnerability and justify the basis for the rating

SCOPE

The following topics will be covered in this unit:

1. Review types of vulnerabilities, especially single-point vulnerabilities and tactics possible under threats/hazards for which there are no mitigation measures.
2. Various approaches and considerations to determine vulnerabilities – Federal Emergency Management Agency, Department of Defense, Department of Justice, and Veterans Affairs.
3. A rating scale and how to use it to determine a vulnerability rating. One or more specific examples will be used to focus students on the following activity.
4. Activity: Identify the vulnerabilities present in the Case Study. As an absolute minimum, consider threats/hazards associated with explosive blast and agents (chemical, biological, and radiological). Determine the vulnerability rating for each asset – threat/hazard pairs of interest.

REFERENCES

1. FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*, Chapter 1
2. Student Manual, Unit IV
3. Case Study – Hazardville Information Company
4. Unit IV visuals

REQUIREMENTS

1. FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings* (one per student)
2. Instructor Guide
3. Student Manual (one per student)
4. Overhead projector or computer display unit
5. Unit IV visuals
6. Chart paper, easel, and markers

UNIT IV OUTLINE

PREPARING TO TEACH THIS UNIT

- **Tailoring Content to the Local Area:** Review the Instructor Notes to identify topics that should focus on the local area. Plan how you will use the generic content, and prepare for a locally oriented discussion.

  The Instructor will discuss generic vulnerabilities found in a building and how tactics possible under threats/hazards can be used against a building. In essence, the students will see the terrorist's thought process used to select a tactic against a target. Conversely, the students will also be presented vulnerabilities that exist for many tactics. Similar to the ratings presented in Units II and III, various approaches to determine vulnerability will be presented.

  One or more specific examples will be used to focus students on the associated student activity. The Instructor will walk through the examples, describing the vulnerability in relation to the Case Study and applying the vulnerability rating approach. The students will be introduced to use of the **Building Vulnerability Assessment Checklist (Table 1-22 of FEMA 426)** during this Unit. Use of the checklist will be reemphasized in Units VIII and IX covering Chapters 2 and 3, respectively, of FEMA 426. Note that the vulnerability rating at

this point in the assessment process is a rapid screening approach. It provides an initial vulnerability rating based upon mitigation measures already in place against the threat/hazard tactic. It is derived from the interview process with the building management and staff to focus the actual vulnerability assessment to be performed later.

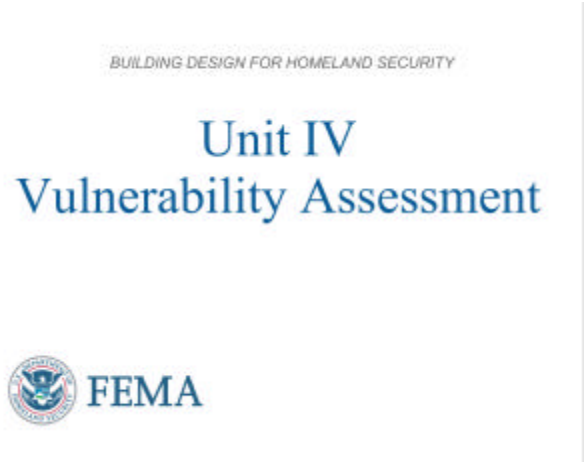
- **Optional Activity:** There are no optional activities in this unit.

- **Activity:** The students will apply the vulnerability identification (or lack of mitigation measures) and vulnerability rating to the Case Study to identify and rate the vulnerabilities found in the Case Study for each asset – threat/hazard pair. The students will quickly review/scan the building data, physical security, building structure, electrical systems, mechanical systems information systems, communications, emergency response, and geographic information system (GIS) portfolio to have a sense of the vulnerabilities at the Hazardville Information Company. The Building Vulnerability Assessment Checklist should also be used to capture the sense of potential vulnerabilities and mitigation measures.

- Refer students to their Student Manuals for worksheets and activities.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

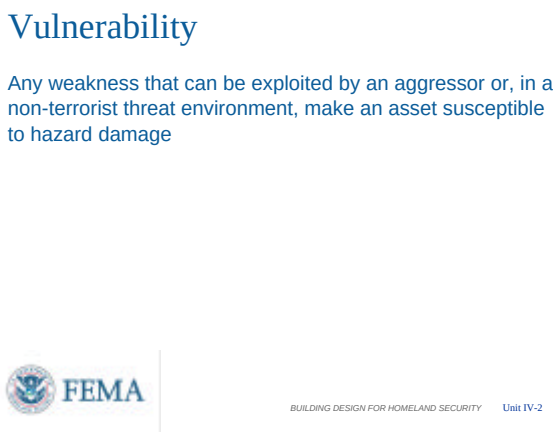
VISUAL IV-1



Introduction and Unit Overview

This is Unit IV Vulnerability Assessment. In this unit, we will review types of vulnerabilities, approaches, and considerations to determine vulnerabilities, review a rating scale, and use the **FEMA 426 Building Vulnerability Assessment Checklist (Table 1-22)** to evaluate the vulnerability against a level of protection standard.

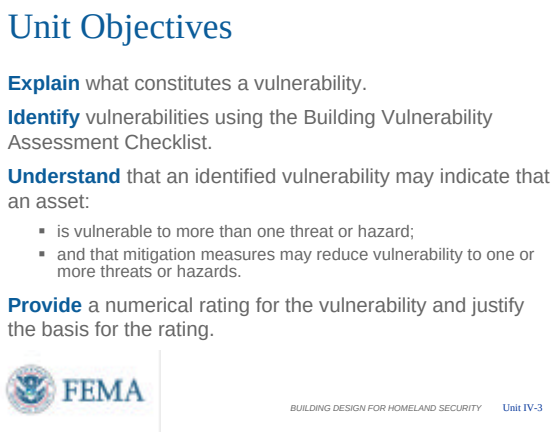
VISUAL IV-2



Vulnerability

The definition of vulnerability is any weakness that can be exploited by an aggressor or, in a non-terrorist threat environment, make an asset susceptible to hazard damage.

VISUAL IV-3



Unit Objectives

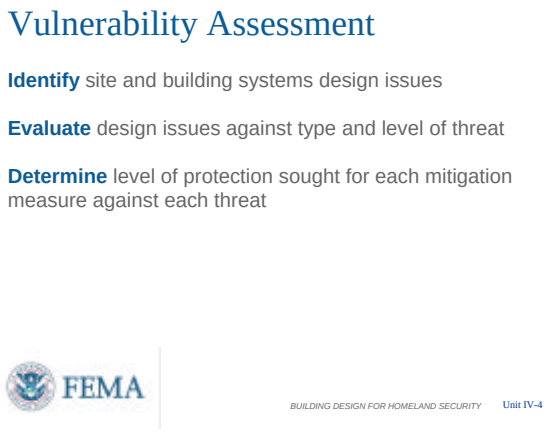
At the end of this unit, you should be able to:

1. Explain what constitutes a vulnerability.
2. Identify vulnerabilities using the Building Vulnerability Assessment Checklist.
3. Understand that an identified vulnerability may indicate that an asset

is vulnerable to more than one threat or hazard, and that mitigation measures may reduce vulnerability to one or more threats or hazards.

4. Provide a numerical rating for the vulnerability and justify the basis for the rating.

VISUAL IV-4



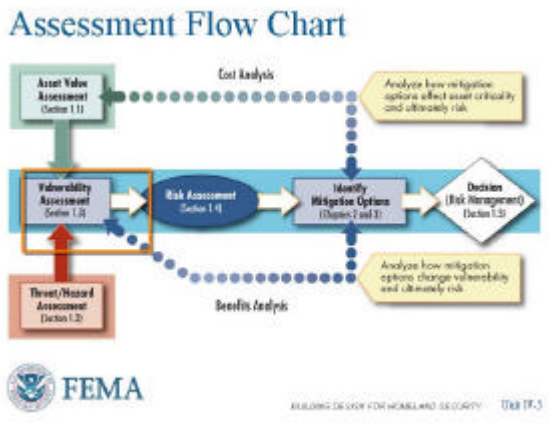
Vulnerability Assessment in this context has three components:

- Identify site and building systems design issues
- Evaluate design issues against type and level of threat
- Determine level of protection sought for each mitigation measure against each threat.

Vulnerability assessments occur at different scales, including:

- State
- Regional
- Site
- Building

VISUAL IV-5



Assessment Flow Chart

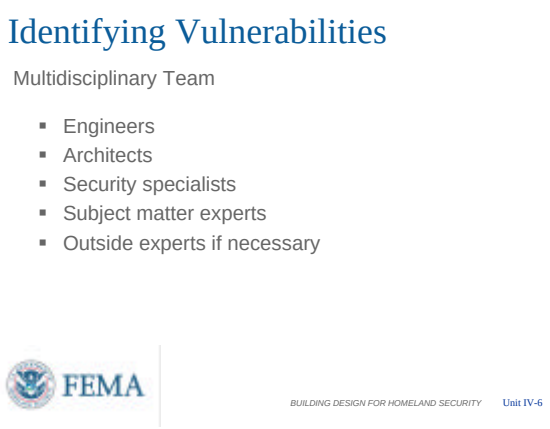
Reviewing the Assessment Flow Chart, the vulnerability assessment is the next step in the risk assessment process.

In the prior steps, assets and their respective values were assigned, the threat was analyzed, a Design Basis Threat was established, and a Level of Protection was selected.

The next step is conduct the vulnerability assessment, which is an in-depth analysis of the building functions, systems, and site characteristics to identify building

weaknesses and lack of redundancy, and determine mitigations or corrective actions that can be designed or implemented to reduce the vulnerabilities.

VISUAL IV-6



Identifying Vulnerabilities

Assessing a building's vulnerabilities requires a multidisciplinary team. It should not be conducted solely by an engineer or by a security specialist. Only a balanced team can have an understanding of the identified aggressors or threat/hazards and how they can affect the building's critical functions and infrastructure. Team members include:

- Engineers
- Architects
- Security specialists
- Subject matter experts
- Outside experts if necessary

Tailor the team to the individual project.

VISUAL IV-7

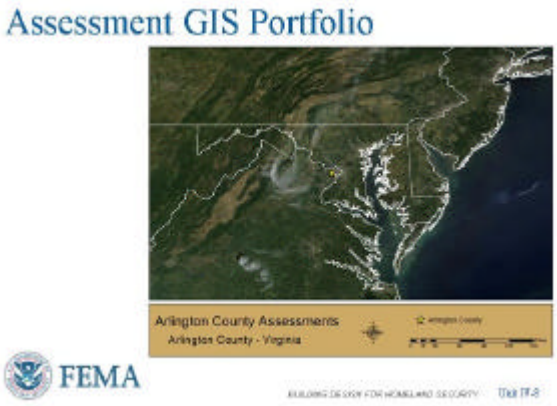
Vulnerability Assessment Preparation

After assembling a team, the assessment process starts with a detailed planning and information collection of the site. If possible, the information should be gathered in a GIS format. Types of coordination with the building stakeholders include:

- Site and Building Plans
- Utilities
- Emergency Plans (shelter, evacuation)
- Interview schedules
- Escorts for building access

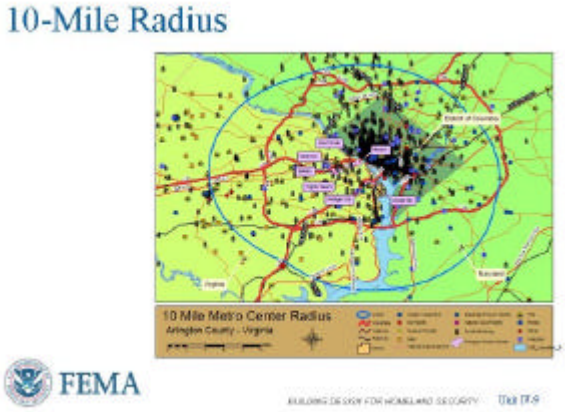
INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL IV-8



Note: For additional information on HAZUS-MH, refer the student to www.HAZUS.org. Another important resource is Geospatial One-Stop (www.geo-one-stop.gov), a one-stop source of geospatial information from across the nation. Geospatial information allows decisions to be viewed in a community context (e.g., showing the geographic components of buildings, lifelines, hazards, etc.).

VISUAL IV-9



Assessment GIS Portfolio

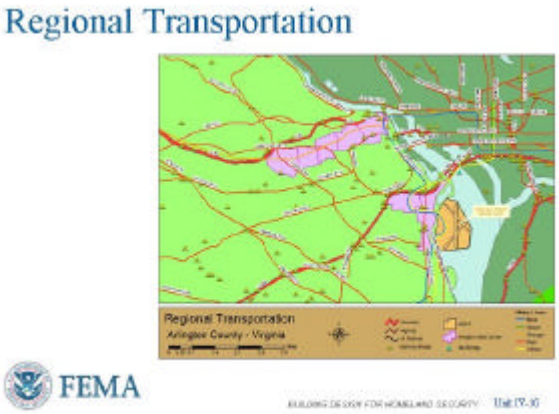
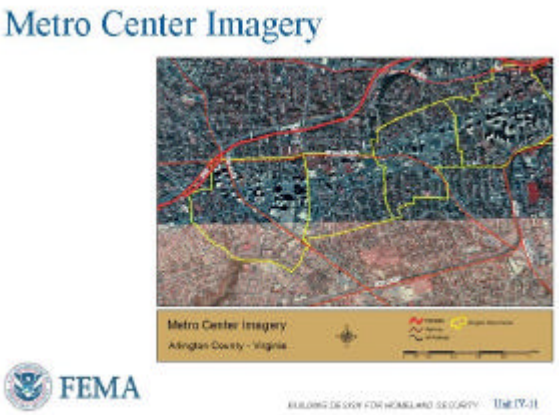
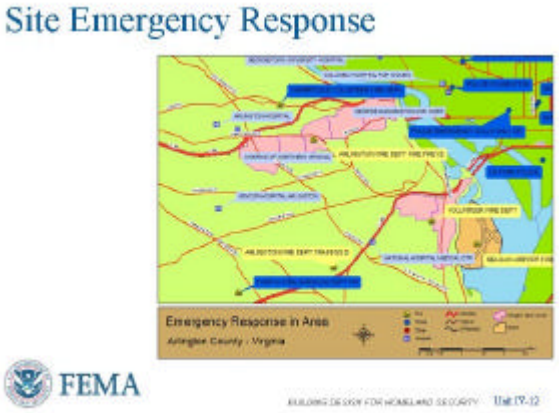
A technique to organize required information is to develop an Assessment GIS Portfolio. The portfolio is designed to support vulnerability and risk assessments through identification of critical infrastructure and nodes within the surrounding area. The data sets are a combination of commercial and government (FEMA – HAZUS-MH, USGS, state, and local data) imagery interpretation, as well as open source transportation, utility, and political boundaries. Portfolios are tailored to each individual site, but they usually consist of the following elements.

This displays a satellite image of the region with state boundaries delineated. This map provides a general overview for user's initial orientation to a site.

The next series of slides shows how GIS can be used to support threat analysis and vulnerability assessments.

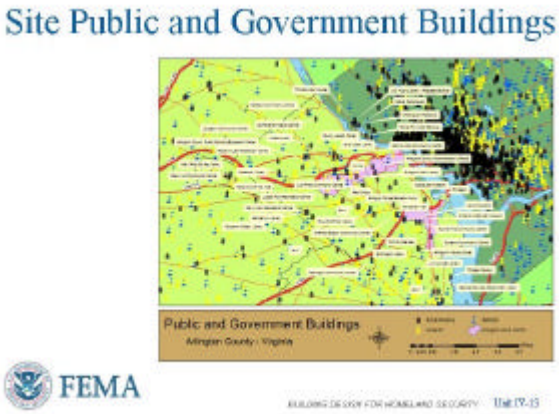
10-Mile Radius

This map displays infrastructure and features within a 10-mile radius that could have an impact on the site. Features mapped include utilities, major transportation networks, first responders, and government facilities.

INSTRUCTOR NOTES	CONTENT/ACTIVITY
VISUAL IV-10 	**Regional Transportation** The regional transportation map can be used for planning evacuation routes and identifying single-point nodes such as bridges and tunnels.
VISUAL IV-11 	**Metro Center Imagery** Imagery provides users with satellite imagery of the region surrounding a site. Commercial, industrial, and residential areas can easily be differentiated, as well as rural and urban areas. This map can be used for an overview of the surrounding area and for determining if collateral damage is a significant risk.
VISUAL IV-12 	**Site Emergency Response** This map displays first responders and hospitals near a site and can be used to estimate response times during an emergency.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

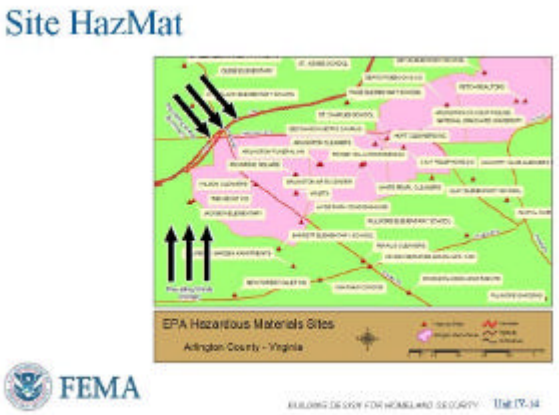
VISUAL IV-13



Site Public/Government Buildings

This map shows the location of government and public buildings in the region, including government facilities, schools, and churches. Government buildings potentially could be the target of terrorist operations. Therefore, the possibility of collateral damage should be considered for sites in close proximity. Additionally, some churches and schools may be designated community shelters and resources during emergencies.

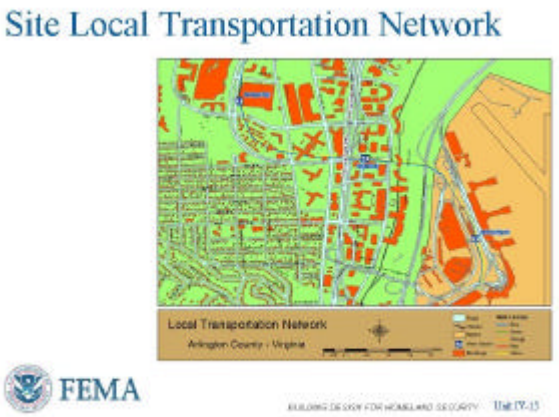
VISUAL IV-14



Site HazMat

This map displays hazardous materials (HazMat) sites tracked by various EPA databases. They include large HazMat sites such as refineries and chemical plants, but also include smaller sites with small quantities of chemicals such as schools and dry cleaners. Some sites that contain very small amounts of HazMat are filtered out Prevailing wind direction from the National Oceanic and Atmospheric Administration (NOAA) Climatic Data Center is shown to help evaluate the vulnerabilities from surrounding hazards that can be used by a terrorist as a weapon.

VISUAL IV-15

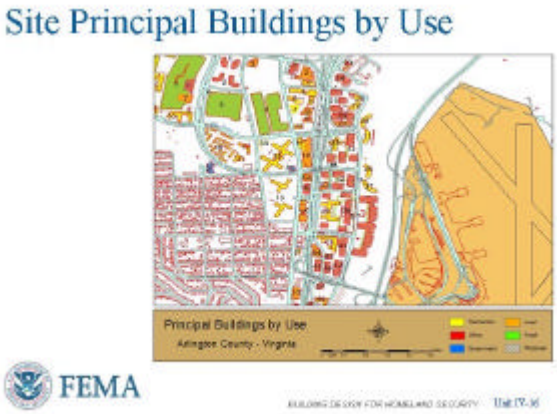


Site Local Transportation Network

The local transportation map provides greater resolution of transportation routes in the local area surrounding a site. It can be used for planning evacuation routes and alternate routes during for an emergency. It also shows proximity to routes that could potentially be used for carrying hazardous materials.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL IV-16



Site Principal Buildings by Use

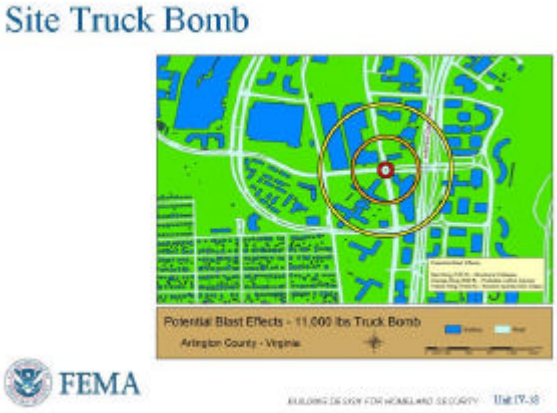
This map provides a quick overview of the primary use of principal buildings surrounding a site. It is useful when conducting threat assessments to help identify potential surrounding terrorist targets and the likelihood of collateral damage.

VISUAL IV-17

Site Perimeter Imagery

Site imagery gives a view of the site and allows assessors to analyze the layout of the site, including site entry points and building separation. The imagery can also be integrated with building plans to provide important information for implementing mitigation measures and making other security decisions.

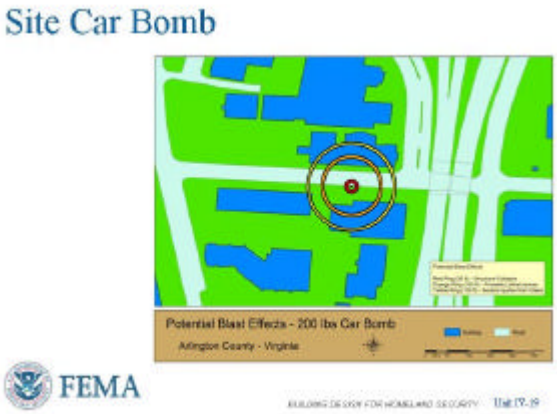
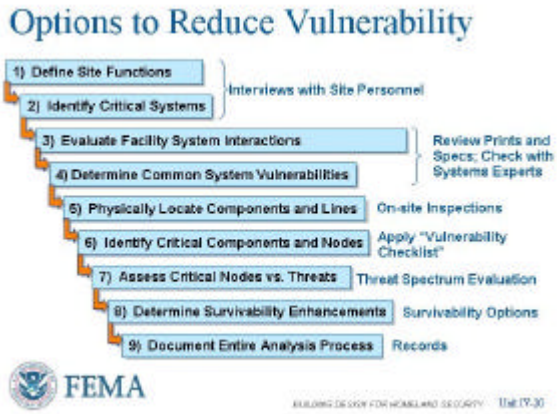
VISUAL IV-18



Site Truck Bomb

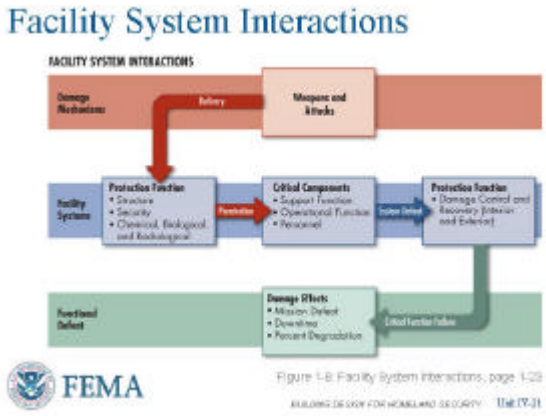
Displays the potential effects of a vehicle bomb assuming a nominal building structure. It is an estimation based on range-to-effects charts and is useful for analyzing vehicular flow and stand-off issues. The results of more accurate site-specific blast analysis can also be used to replace the nominal estimations.

This is an example of the potential blast effects associated with a truck bomb.

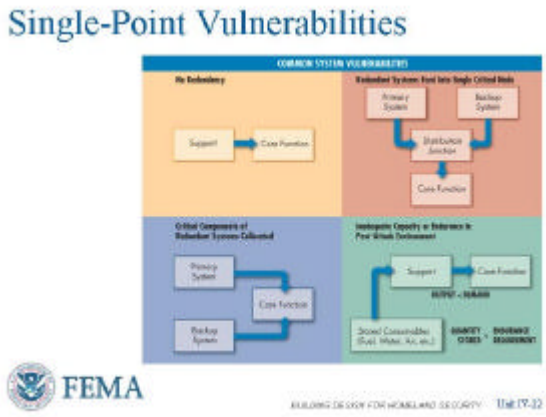
INSTRUCTOR NOTES	CONTENT/ACTIVITY
VISUAL IV-19  	**Site Car Bomb** This is an example of the potential blast effects associated with a car bomb.
VISUAL IV-20  	**Options to Reduce Vulnerability** After identifying and collecting information on the site, the multidisciplinary team follows the nine steps listed here: 1. Define Site Functions 2. Identify Critical Systems 3. Evaluate Facility System Interactions 4. Determine Common System Vulnerabilities 5. Physically Locate Components and Lines 6. Identify Critical Components and Nodes 7. Assess Critical Nodes Versus Threats 8. Determine Survivability Enhancements (and Options) 9. Document Entire Analysis Process This process is explained in more detail in FEMA 452, "*Methodology for Preparing Threat Assessments For Commercial Buildings*." For this course, this is an overview of what a more detailed on-site assessment should accomplish. As part of the Case Study, this process will be led by the instructor and the students will identify the vulnerabilities and mitigation options.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL IV-21



VISUAL IV-22



Exam Questions #A4 and B3

Single-Point Vulnerabilities are critical functions or systems that lack redundancy and, if damaged by an attack, would result in immediate organization disruption or loss of capability.

Facility System Interactions

Every building or facility can be attacked and damaged or destroyed as illustrated in the flow chart.

A terrorist selects the weapon and tactic that will destroy the building or infrastructure target.

At a site with multiple buildings, **Tables 1-6 through 1-16 in FEMA 426** can be used to rank order these buildings and thus to determine which buildings require more in-depth analysis.

Single-Point Vulnerabilities (SPVs)

The function and infrastructure analysis will identify the geographic distribution within the building and interdependencies between critical assets. Ideally, the functions should have geographic dispersion as well as a recovery site or alternate work location. However, some critical building functions and infrastructure do not have a backup, or will be found collocated. This design creates what is called a Single-Point Vulnerability.

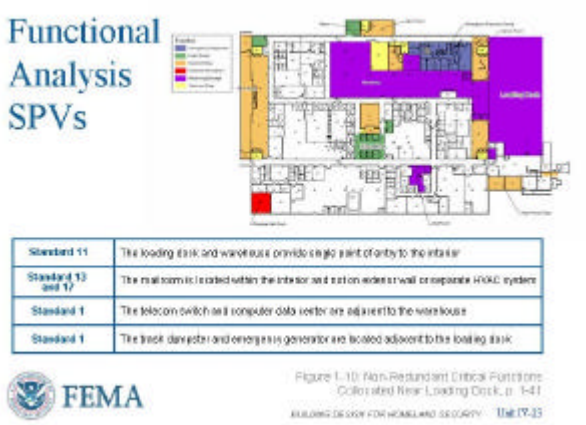
Identification and protection of these Single-Point Vulnerabilities is a key aspect of the assessment process.

This chart provides examples of this concept:

1. No Redundancy
2. Redundant Systems Feed Into Single Critical Node
3. Critical Components of Redundant Systems Collocated
4. Inadequate Capacity or Endurance in Post-Attack Environment

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL IV-23



Functional Analysis SPVs

There are both Functional Analysis SPVs and Infrastructure SPVs.

Functional Analysis SPVs are depicted in this chart. This figure shows an example of a building that has numerous critical functions and infrastructure collocated, which creates a single-point vulnerability.

VISUAL IV-24

Infrastructure Analysis SPVs

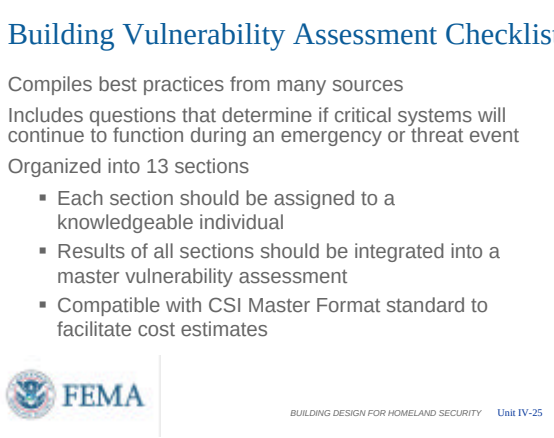
Typical infrastructure SPVs are depicted here:

- Air intakes at ground level
- Ground level drive through drop-off atrium with no anti-vehicle barrier
- Single primary electrical service
- Single telecom switch room in parking garage

Many commercial buildings have collocated electrical, mechanical, and telecom rooms that share a common central distribution core or chase.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL IV-25

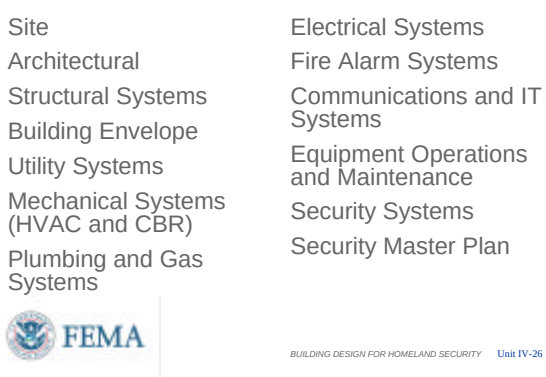


The Building Vulnerability Assessment Checklist is based on a checklist developed by the Department of Veterans Affairs (VA). The checklist can be used as a screening tool for preliminary design vulnerability assessment. In addition to examining design issues that affect vulnerability, the checklist includes questions that determine if critical systems continue to function in order to enhance deterrence, detection, denial, and damage limitation, and to ensure that emergency systems function during a threat or hazard situation.

Building Vulnerability Assessment Checklist

FEMA 426 provides the **Building Vulnerability Assessment Checklist (Table 1-22)**, which compiles many best practices based on technologies and scientific research to consider during the design of a new building or renovation of an existing building, and help guide the multidisciplinary team through the vulnerability analysis. It allows a consistent security evaluation of designs at various levels.

VISUAL IV-26

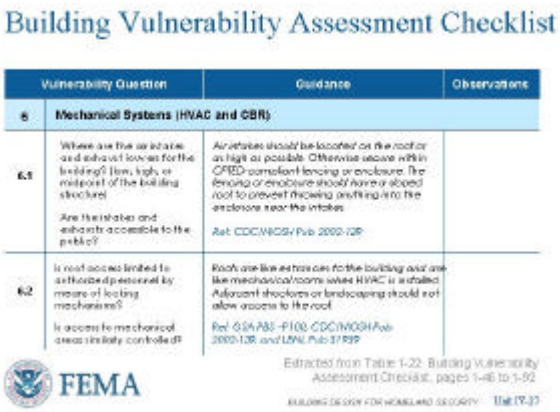


Building Vulnerability Assessment Checklist

To conduct a vulnerability assessment of a building or preliminary design, each section of the checklist should be assigned to an engineer, architect, or subject matter expert who is knowledgeable and qualified to perform an assessment of the assigned area.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

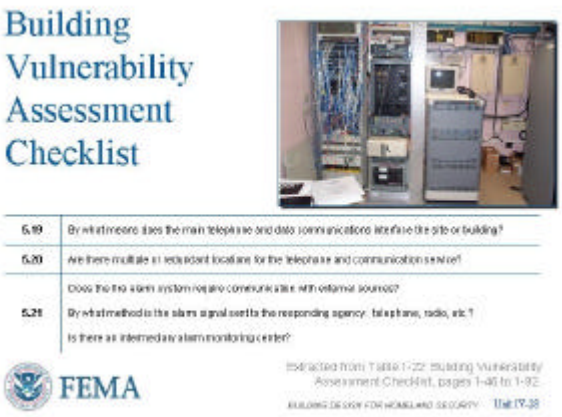
VISUAL IV-27



Building Vulnerability Assessment Checklist

Each assessor should consider the questions and guidance provided to help identify vulnerabilities and document results in the observations column. Not all possible questions are in the checklist, but it provides a good basis to guide the assessment.

VISUAL IV-28



Building Vulnerability Assessment Checklist

Notice that the checklist leads assessment team members to see the same critical functions or infrastructure from different perspectives.

For example, here a parking lot is analyzed by questions from both the site and building envelope sections.

This cross analysis is one of the strengths of the methodology.

VISUAL IV-29

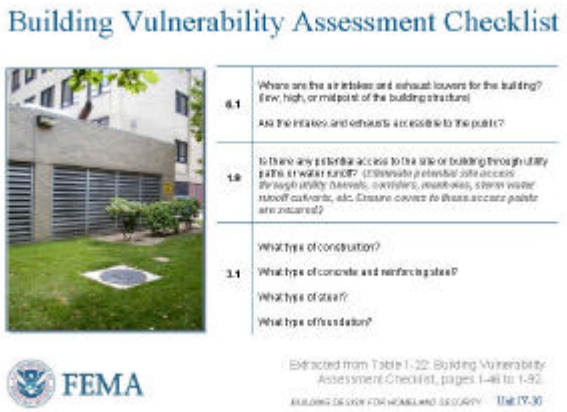
Building Vulnerability Assessment Checklist

In this example, the same feature, a loading dock, is addressed by different sections.

The location of the trash dumpster, building overhang, and exposed loading dock columns make this area susceptible to significant blast damage.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

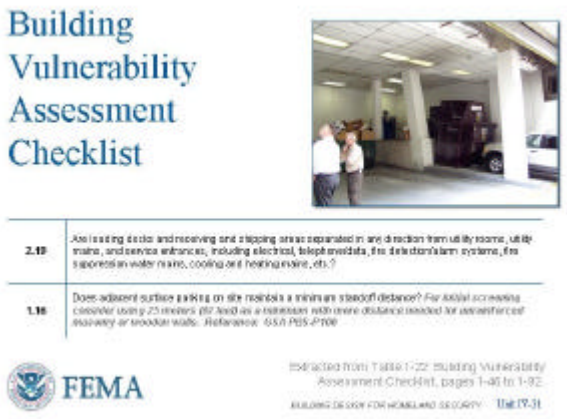
VISUAL IV-30



Building Vulnerability Assessment Checklist

In this example, the same feature, an air intake, is addressed by questions from three sections: #1 – Site; #3 – Structural Systems; #6 – Mechanical Systems.

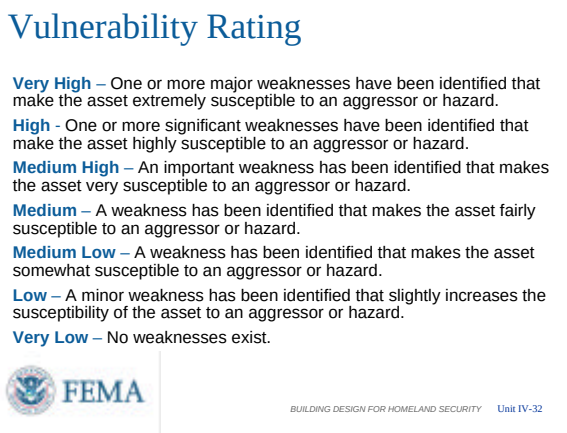
VISUAL IV-31



Building Vulnerability Assessment Checklist

Section 5 of the Building Vulnerability Assessment Checklist addresses Utility Systems. The results of Utility Systems vulnerability assessments and the other 12 categories provide a basis for determining vulnerability ratings for the facility.

VISUAL IV-37



Vulnerability Rating

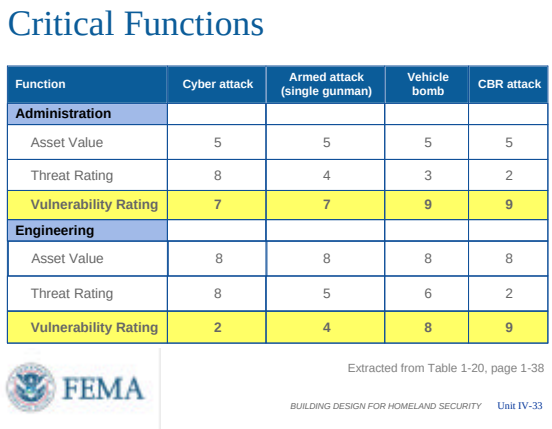
The results of the 13 assessment sections should be integrated into a master vulnerability assessment in order to provide the basis for determining vulnerability rating numeric values.

In the rating scale of 1 to 10, 1 means very low or no weaknesses exist, and 10 means one or more major weaknesses exist to make an asset extremely susceptible to an aggressor.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

- **Very High** – One or more major weaknesses have been identified that make the asset extremely susceptible to an aggressor or hazard.
- **High** – One or more significant weaknesses have been identified that make the asset highly susceptible to an aggressor or hazard.
- **Medium High** – An important weakness has been identified that makes the asset very susceptible to an aggressor or hazard.
- **Medium** – A weakness has been identified that makes the asset fairly susceptible to an aggressor or hazard.
- **Medium Low** – A weakness has been identified that makes the asset somewhat susceptible to an aggressor or hazard.
- **Low** – A minor weakness has been identified that slightly increases the susceptibility of the asset to an aggressor or hazard.
- **Very Low** – No weaknesses exist.

VISUAL IV-33



Critical Functions Matrix

The Vulnerability Rating is entered into the same site critical functions matrix and the site critical infrastructure matrix that we saw in Units II and III.

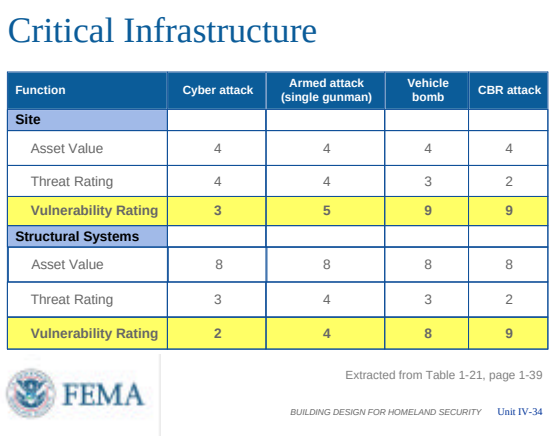
The site Critical Functions matrix lists functions down the left side and threats across the top.

The Vulnerability Rating under the Engineering Function and Threat Pairs functions is highlighted. A medium and

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

The Vulnerability Rating is subjective and the assessor has to take into account how important the asset is to the overall mission, how well it is protected or how quickly it can be replaced, and what tactics and weapons are effective against the asset.

VISUAL IV-34



VISUAL IV-35

high Vulnerability Rating (5) was assigned to the Administration Function threat pairs to illustrate an exposed function near exterior walls and entrances. A range of ratings was assigned for the Engineering Function threat pairs to illustrate a function that is typically in the interior core, but shares common HVAC systems and is likely within a blast damage zone.

Critical Infrastructure Matrix

The site Critical Infrastructure matrix lists Infrastructure down the left side and threats across the top.

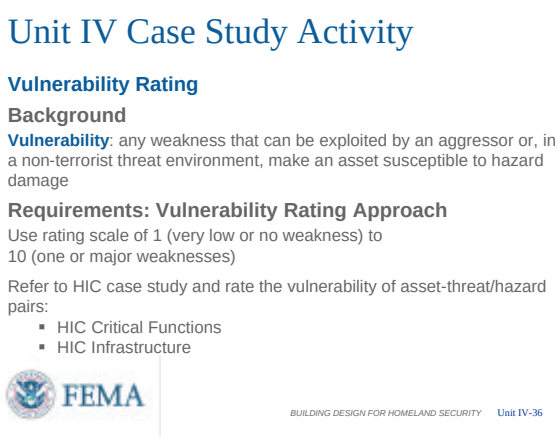
The Vulnerability Rating under the Site and Structural Systems is highlighted. A range of Vulnerability Rating values from medium to high were assigned for the Site Infrastructure threat pairs to illustrate the first layer of defense and aerial extent that can be affected. A range of Vulnerability Rating values from medium to high were assigned for the Structural System threat pairs to illustrate impact on the structure in the second layer of defense.

Summary

- Identify core functions and Critical Infrastructure
- Assign a building's assets or resources a value
- Apply ranking to the Critical Site Functional matrix and the Critical Site Infrastructure System Matrix

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL IV-36



Refer participants to the Unit IV Case Study activity in the Student Manual.

Members of the instructor staff should be available to answer questions and assist groups as needed.

At the end of the working sessions, reconvene the class and facilitate group reporting.

Student Activity

Vulnerability is any weakness that can be exploited by an aggressor or, in a non-terrorist threat environment, make an asset susceptible to hazard damage.

DISCUSSION QUESTION

Determine what if any vulnerability exists in the building design?

Suggested Responses:

- *Critical functions or systems that lack redundancy and if damaged would result in immediate organization disruption or loss of capability ("Single-Point Vulnerability").*
- *Redundant systems feeding into a single critical node.*
- *Critical components of redundant systems collocated.*
- *Inadequate capacity or endurance in post-attack environment.*

Vulnerability rating requires identifying and rating the vulnerability of each asset-threat pair.

In-depth vulnerability assessment of a building evaluates specific design and architectural features and identifies all vulnerabilities of the building functions and building systems.

Activity Requirements: Selected Building Systems Example

- Working in small groups, answer the worksheet questions and record relevant observations regarding the HIC Building Systems.

INSTRUCTOR NOTES	CONTENT/ACTIVITY
	• Also determine what, if any, vulnerability exists. Take 15 minutes to complete this part of the activity. **Vulnerability Rating Approach** Using a rating scale of 1 to 10, 1 means very low or no weaknesses exist, and 10 means one or more major weaknesses exist to make an asset extremely susceptible. In a Vulnerability Assessment rating, vulnerability is rated by assessing available information to identify the most obvious areas of vulnerability that need to be assessed in depth as is illustrated in the building systems example. **Activity Requirements: HIC Critical Functions and Infrastructure Vulnerability Ratings** Continue working in small groups. Refer to the HIC Case Study and rate the vulnerability of the asset-threat/hazard pairs for: • HIC Critical Functions • HIC Infrastructure Students take 20 minutes to complete the Site, Architectural and Envelope ratings of the Critical Infrastructure matrix. Solutions will be reviewed in plenary group. **Transition** Unit V will cover Risk Assessment/ Risk Management. Unit VI will cover Explosive Blast.

UNIT IV CASE STUDY ACTIVITY: VULNERABILITY RATING

Vulnerability is any weakness that can be exploited by an aggressor or, in a non-terrorist threat environment, make an asset susceptible to hazard damage. Vulnerabilities may include:

- Critical functions or systems that lack redundancy and if damaged would result in immediate organization disruption or loss of capability ("Single-Point Vulnerability")
- Redundant systems feeding into a single critical node
- Critical components of redundant systems collocated
- Inadequate capacity or endurance in post-attack environment

Vulnerability rating requires identifying and rating the vulnerability of each asset-threat pair. In-depth vulnerability assessment of a building evaluates specific design and architectural features and identifies all vulnerabilities of the building functions and building systems.

Requirement

For an example of how a specific asset is assessed, answer the following questions and record relevant observations on the following table regarding the HIC site and building. Determine what, if any. vulnerability exists:

Section	Vulnerability Questions	Guidance	Observations
1.16	Does adjacent surface parking on site maintain a minimum stand-off distance?	The specific stand-off distance needed is based upon the design basis threat bomb size and the building construction. For initial screening, consider using 25 meters (82 feet) as a minimum, with more distance needed for unreinforced masonry or wooden walls. Reference: *GSA PBS-100*	There is no adjacent parking per se, but there is one parking lot or area that any tenant or visitor to the office park can use. Stand-off distance to the front parking lot is less than the 82 feet screening value. Cars or trucks can drive up to the loading dock in the rear.
1.19	Do site landscaping and street furniture provide hiding places?	Minimize concealment opportunities by keeping landscape plantings (hedges, shrubbery, and large plants with heavy ground cover) and street furniture (bus shelters, benches, trash receptacles, mailboxes, newspaper vending machines) away from the building to permit observation of intruders and prevent hiding of packages. If mail or express boxes are used, the size of the openings should be	There is no street furniture shown for this building. The landscaping shown is grass and trees are mature/tall enough so that a package cannot be hidden at the base. The hedge along the building drip line may conceal a package, if allowed to get taller or denser. There is

		restricted to prohibit the insertion of packages. Reference: *GSA PBS-100*	no mail or express box and there is no slot in the glass main entrance door. Due to the size of the building columns, a package could be overlooked.
2.15	Are critical assets (people, activities, building systems and components) located close to any main entrance, vehicle circulation, parking, maintenance area, loading dock, or interior parking? Are the critical building systems and components hardened?	Critical building components include: emergency generator, including fuel systems, day tank, fire sprinkler, and water supply; normal fuel storage; main switchgear; telephone distribution and main switchgear; fire pumps; building control centers; uninterruptible power supply (UPS) systems controlling critical functions; main refrigeration and ventilation systems if critical to building operation; elevator machinery and controls; shafts for stairs, elevators, and utilities; and critical distribution feeders for emergency power. Evacuation and rescue require emergency systems to remain operational during a disaster and they should be located away from attack locations. Primary and back-up systems should be separated to reduce the risk of both being impacted by a single incident if collocated. Utility systems should be located at least 50 feet from loading docks, front entrances, and parking areas. One way to harden critical building systems and components is to enclose them within hardened walls, floors, and ceilings. Do not place them near high risk areas where they can receive collateral damage. Reference: *GSA PBS-100*	This building is not large enough to maintain separation distances. Attack from the front of the building primarily impacts office space. Attack from the rear affects critical utilities and, through the loading dock area, the heart of the company – the computer center. No critical components are hardened as seen by the natural gas and electric service to the building. The UPS, mechanical and electrical room, and the diesel generator can be affected by a single bomb less than 50 feet from all these areas or taken out by a single wayward truck.
2.16	Are high value or critical assets located as far into the interior of the building as possible and separated from the public areas of the building?	Critical assets, such as people and activities, are more vulnerable to hazards when on an exterior building wall or adjacent to uncontrolled public areas inside the building. Reference: *GSA PBS-100*	People are located along the exterior wall at the front of the building. The secure space has the best interior space location – not on an exterior wall, as does the conference room.

			The office space acts as the buffer between the critical functions in the back and the public area of the building at the main entrance.
4.2	Is there less than 40 percent fenestration openings per structural bay? Is the window system design on the exterior façade balanced to mitigate the hazardous effects of flying glazing following an explosive event? (glazing, frames, anchorage to supporting walls, etc.)	The performance of the glass will similarly depend on the materials. Glazing may be single pane or double pane, monolithic or laminated, annealed, heat strengthened, or fully tempered. The percent fenestration is a balance between protection level, cost, the architectural look of the building within its surroundings, and building codes. One goal is to keep fenestration to below 40 percent of the building envelope vertical surface area, but the process must balance differing requirements. A blast engineer may prefer no windows; an architect may favor window curtain walls; building codes require so much fenestration per square footage of floor area; fire codes require a prescribed window opening area if the window is a designated escape route; and the building owner has cost concerns. Ideally, an owner would want 100 percent of the glazed area to provide the design protection level against the postulated explosive threat (design basis threat – weapon size at the expected stand-off distance). However, economics and geometry may allow 80 percent to 90 percent due to the statistical differences in the manufacturing process for glass or the angle of incidence of the blast wave upon upper story windows (4th floor and higher). Reference: *GSA PBS-100*	Windows are only used in the office space area of the building. While dimensions are not given, it looks like the glass is at least 40 percent of the wall area between building structural columns. The window system is a standard commercial installation and thus, the glass, framing, and anchorage are expected to be insufficient for the design basis threat at the available stand-off. One benefit is that there are windows only on two sides of the building.

HIC Critical Functions Vulnerability Rating

Requirement

Refer to the HIC Case Study and rate the vulnerability of the following asset-threat/hazard pairs.

Function	Cyber Attack	Armed Attack	Vehicle Bomb	CBR Attack
1. Administration	8	8	8	8
2. Engineering/IT Technicians	8	8	8	8
3. Loading Dock/ Warehousing	2	3	8	8
4. Data Center	9	3	8	8
5. Communications	8	3	8	8
6. Security	3	3	8	8
7. Housekeeping	1	1	8	8

HIC Infrastructure Vulnerability Rating

Refer to the HIC Case Study and rate the vulnerability of the following asset-threat/hazard pairs.

Function	Cyber Attack	Armed Attack	Vehicle Bomb	CBR Attack
1. Site	3	8	8	8
2. Architectural	3	8	8	4
3. Structural Systems	3	8	8	3
4. Envelope Systems	3	8	8	3
5. Utility Systems	5	7	6	3
6. Mechanical Systems	5	7	8	7
7. Plumbing and Gas Systems	3	8	8	5

8. Electrical Systems	5	7	8	5
9. Fire Alarm Systems	3	3	8	3
10. IT/Communications Systems	10	8	8	6

Unit V

COURSE TITLE Building Design for Homeland Security

TIME 75 minutes

UNIT TITLE Risk Assessment/Risk Management

OBJECTIVES

1. Explain what constitutes risk
2. Evaluate risk using the Threat-Vulnerability Matrix to capture assessment information
3. Provide a numerical rating for risk and justify the basis for the rating
4. Identify top risks for asset – threat/hazard pairs that should receive measures to mitigate vulnerabilities and reduce risk

SCOPE

The following topics will be covered in this unit:

1. Definition of risk and the various components to determine a risk rating.
2. The FEMA 426 approach to determining risk.
3. A rating scale and how to use it to determine a risk rating. One or more specific examples will be used to focus students on the following activity.
4. The relationships between high risk, the need for mitigation measures, and the need to identify a Design Basis Threat and Level of Protection.
5. Activity: Determine the risk rating for the asset – threat/hazard pairs of interest. Identify the top three risk ratings for the Case Study.

REFERENCES

1. FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*, Chapter 1
2. Student Manual, Unit V
3. Case Study – Hazardville Information Company
4. Unit V visuals

REQUIREMENTS

1. FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings* (one per student)
2. Instructor Guide
3. Student Manual (one per student)
4. Overhead projector or computer display unit

5. Unit V visuals
6. Chart paper, easel, and markers

UNIT V OUTLINE

PREPARING TO TEACH THIS UNIT

- **Tailoring Content to the Local Area:** Review the Instructor Notes to identify topics that should focus on the local area. Plan how you will use the generic content, and prepare for a locally oriented discussion.

  The Instructor will begin this unit with a brief discussion of terrorism and technological hazards worldwide and within the United States. The probability of natural hazards and how they are considered during design will be compared to the probability of manmade hazards, both terrorism and technological accidents. This sets the stage for identifying where to get information about threats and hazards.

  Next, the Instructor will use FEMA 386-7 to describe the spectrum of tactics or events that can occur. This leads into the five components used to define a threat (or hazard) and one interpretation of the Homeland Security Advisory System.

  Various threat and vulnerability rating systems will be discussed to understand the different methodologies and their applicability to different situations. A simplified threat rating approach will be presented that can be used for new construction or major renovation. This FEMA 426 approach forms the basis of the Unit V student activity.

  The Instructor will use one threat/hazard example from the Case Study to focus students on the student activity. The Instructor will walk through the example, describing the threat and the threat rating approach.

The students will then apply these techniques (threat identification, threat description, and threat rating) to the Case Study to identify and rate the threat from explosive blast and agents (chemical, biological, and radiological). Note that these event profiles can result from terrorism or technological hazards.

The Instructor will define risk by its components and the different approaches used to determine risk. One or more examples will be used to show the students how to determine and evaluate the risk rating for each asset – threat/hazard pair in the threat-vulnerability matrix. The Instructor will also discuss the relationship between an identified high risk asset – threat/hazard pair and the need for mitigation measures to reduce that risk by reducing the vulnerability rating. Finally, the value of providing a Design Basis Threat and Desired Level of Protection will be presented. The Design Basis Threat and Desired Level of Protection are needed to allow designers to build the building to withstand the threats. Without the Design Basis Threat or Level of Protection, the building owner would have to provide specific building material specifications to the designer to achieve the Level of Protection for the perceived threat or the designer must provide an educated guess to the building owner for his/her acceptance or rejection.

- **Optional Activity:** There are no optional activities in this unit.

- **Activity:** The student activity is primarily a math exercise in multiplying threat, asset value, and vulnerability ratings to determine the risk rating and then compare it against the risk rating scale. The top three risks should receive additional emphasis during an actual vulnerability assessment to validate the risk by identifying vulnerabilities and as an input to select mitigation measures.

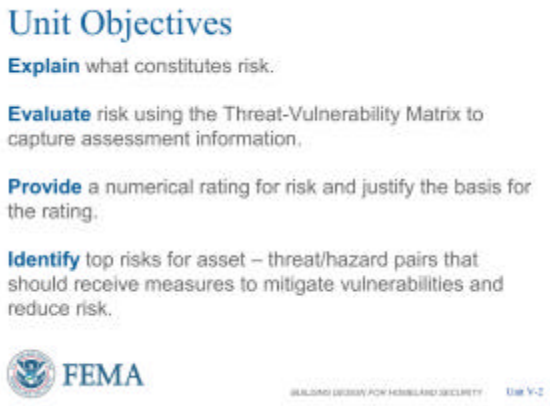
- Refer students to their Student Manuals for worksheets and activities.

INSTRUCTOR NOTES	CONTENT/ACTIVITY
VISUAL V-1	**Introduction and Unit Overview**

This is Unit V Risk Assessment/Risk Management. The Unit will provide a definition of risk and the various components to determine a risk rating, review various approaches to determine risk, review a rating scale, and demonstrate how to use the scale to determine a risk rating.

VISUAL V-2

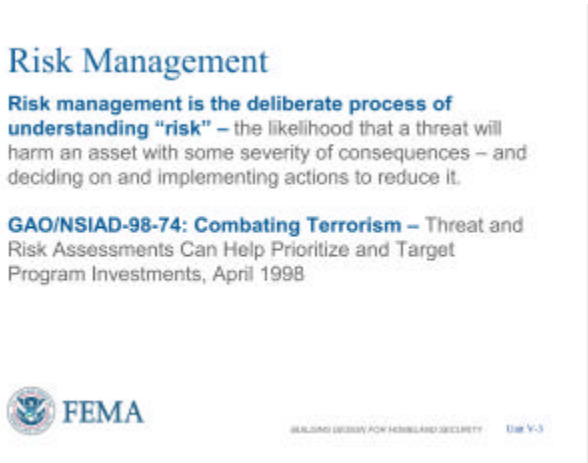
Unit Objectives

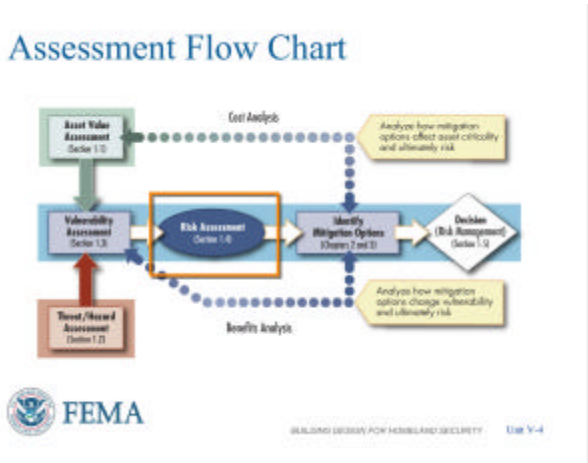


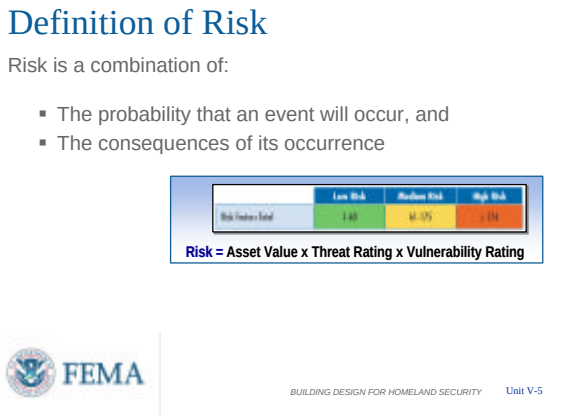
At the end of this unit, you should be able to:

1. Explain what constitutes risk.
2. Evaluate risk using the Threat-Vulnerability Matrix to capture assessment information.
3. Provide a numerical rating for risk and justify the basis for the rating.
4. Identify top risks for asset – threat/hazard pairs that should receive measures to mitigate vulnerabilities and reduce risk.

INSTRUCTOR NOTES	CONTENT/ACTIVITY
VISUAL V-3	**Risk Management** Risk management incorporates an understanding of the vulnerability of assets to the consequences of threats and hazards. The objective is to reduce the vulnerability of assets through mitigation actions.
VISUAL V-4	**Assessment Flow Chart** Reviewing the Assessment Flow Chart, the determination of quantitative values for the risk assessment is the next step in the risk assessment process.
VISUAL V-5	**Risk** Risk can be defined as the potential for a loss or damage to an asset. It takes into account the **value of an asset**, the **threats or hazards** that potentially impact the asset, and the **vulnerability** of the asset to the threat or hazard. Values can be assigned to these three components of risk to provide a risk rating.

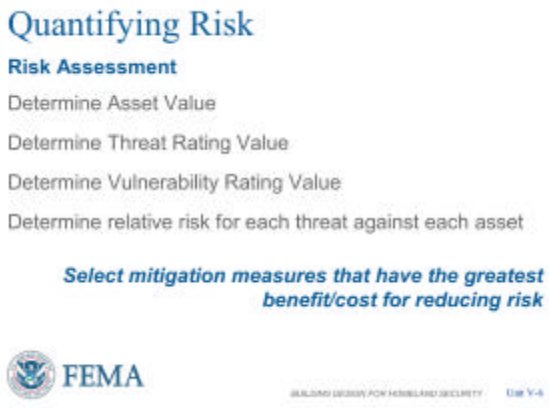




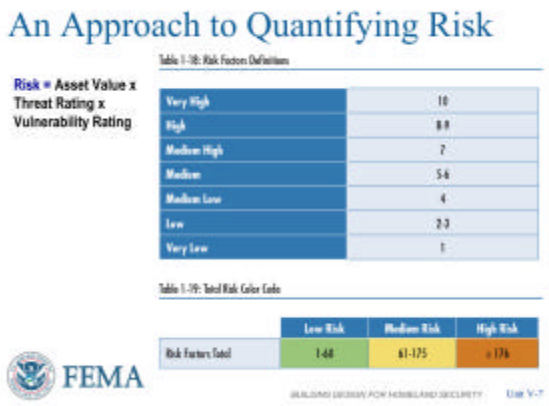


INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL V-6



VISUAL V-7



Exam Questions #A5 and B5

Quantifying Risk

There are at least four steps or **required tasks** in the risk assessment process. A determination of the *Asset Value*, *Threat Rating Value*, *Vulnerability Rating Value*, and identifying or recommending appropriate *mitigation measures to reduce the risk.*

Determining the relative risk of threat against asset justifies the use of limited resources to reduce the greatest risk and focuses the mitigation measures needed.

An Approach to Quantifying Risk

The risk assessment analyzes the threat, asset value, and vulnerability to ascertain the **level of risk** for each critical asset against each applicable threat.

An understanding of risk levels enables the owner of assets to prioritize and implement appropriate mitigation measures, paying particular attention to high consequence threats, to achieve the desired level of protection.

A simplified approach to quantifying risk is shown here. Values can be assigned to asset value/criticality **(see Tables 1-2, 1-9, and 1-10, FEMA 426)**, the threat or hazard, and Vulnerability of the asset to the threats, and numerical scores can be determined that depict relative risk of these assets to manmade hazards.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL V-8

Critical Functions

Function	Cyber attack	Armed attack (single gunman)	Vehicle bomb	CBR attack
Administration	**280**	**140**	**135**	**90**
Asset Value	5	5	5	5
Threat Rating	8	4	3	2
Vulnerability Rating	7	7	9	9
Engineering	**128**	**160**	**384**	**144**
Asset Value	8	8	8	8
Threat Rating	8	5	6	2
Vulnerability Rating	2	4	8	9

FEMA

BUILDING DESIGN FOR HOMELAND SECURITY Unit V-8

Critical Functions Matrix

This analysis completes the site critical functions matrix and the site critical infrastructure matrix that we saw in Units II, III, and IV.

The risk formula is applied and the numeric values color coded as discussed on the previous slide. The color code helps visualize the functions and infrastructure that are vulnerable and the scale helps to identify those areas for in-depth mitigation measures analysis.

The risk ratings under the Administration and Engineering and functions are highlighted. The numeric values result in Medium and High risk ratings for the Functions threat pairs.

VISUAL V-9

Critical Infrastructure

Function	Cyber attack	Armed attack (single gunman)	Vehicle bomb	CBR attack
Site	**48**	**80**	**108**	**72**
Asset Value	4	4	4	4
Threat Rating	4	4	3	2
Vulnerability Rating	3	5	9	9
Structural Systems	**24**	**32**	**240**	**16**
Asset Value	8	8	8	8
Threat Rating	3	4	3	2
Vulnerability Rating	2	4	8	9

FEMA

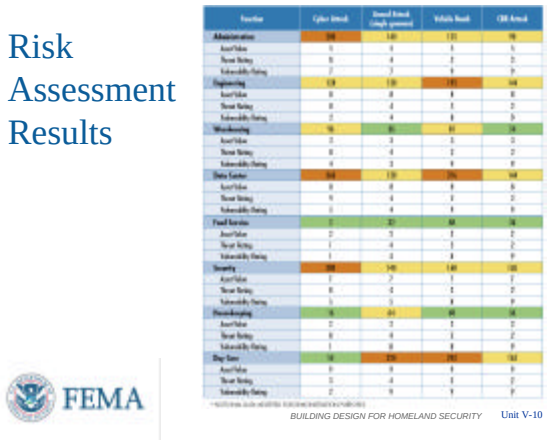
BUILDING DESIGN FOR HOMELAND SECURITY Unit V-9

Critical Infrastructure Matrix

The risk ratings under the Site and Structural Systems are highlighted. The numeric values result in Low to Medium risk ratings for the Infrastructure threat pairs.

INSTRUCTOR NOTES | **CONTENT/ACTIVITY**

VISUAL V-10

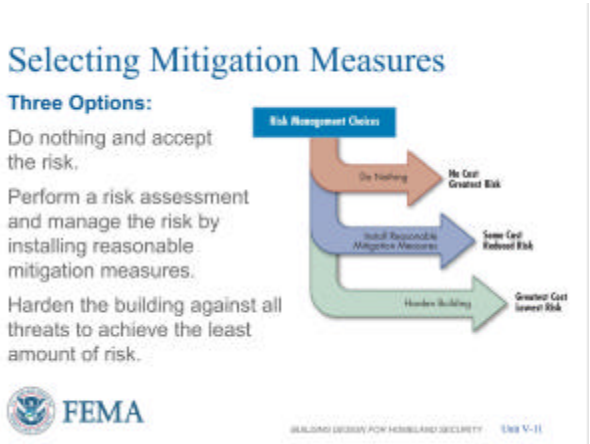


Risk Assessment Results

The process is continued for all the threat – asset pairs. This is a nominal example of a completed risk table.

The risk assessment results in a prioritized list of risks (i.e., threat-asset-vulnerability combinations) that can be used to select safeguards to reduce vulnerabilities (and risk) and create a certain level of protection.

VISUAL V-11



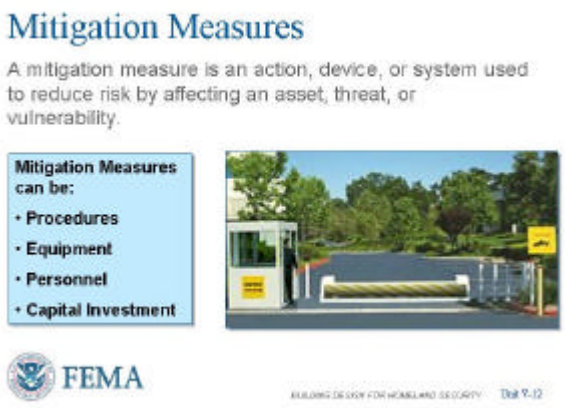
Selecting Mitigation Measures

In every design and renovation project, the owner ultimately has three choices when addressing the risk posed by terrorism. They can:

1. Do nothing and accept the risk (no cost).
2. Perform a risk assessment and manage the risk by installing reasonable mitigation measures (some cost).
3. Harden the building against all threats to achieve the least amount of risk (greatest cost).

Exam Questions #A7 and B8

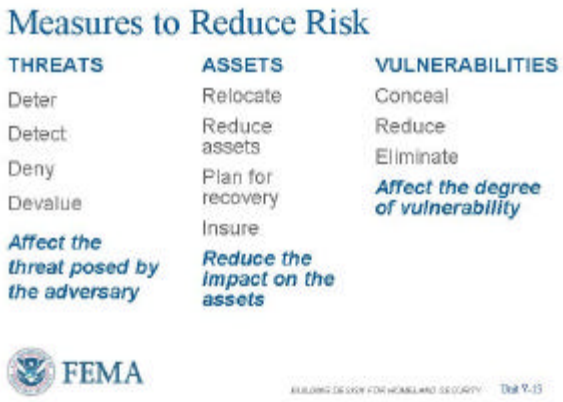
VISUAL V-12



Mitigation Measures

After determining how specific threats potentially impact an asset (and occupants), the architect and building engineer can work with security and risk specialists to identify mitigation measures to reduce risk. Because it is not possible to completely eliminate risk, it is important to determine what level of protection is desirable, and the options for achieving this level through risk management.

INSTRUCTOR NOTES	CONTENT/ACTIVITY
VISUAL V-13	**Measures to Reduce Risk**



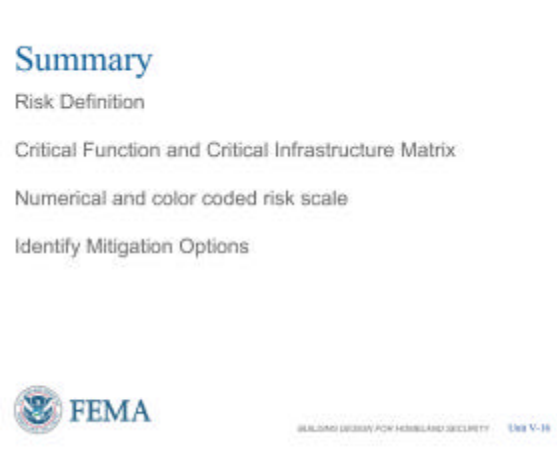
Higher risk hazards require mitigation measures to reduce risk. Mitigation measures are conceived by the design professional and are best incorporated into the building architecture, building systems, and operational parameters, with consideration for life-cycle costs.

In some cases, mitigation measures to enhance security may be in conflict with other design intentions.

VISUAL V-14

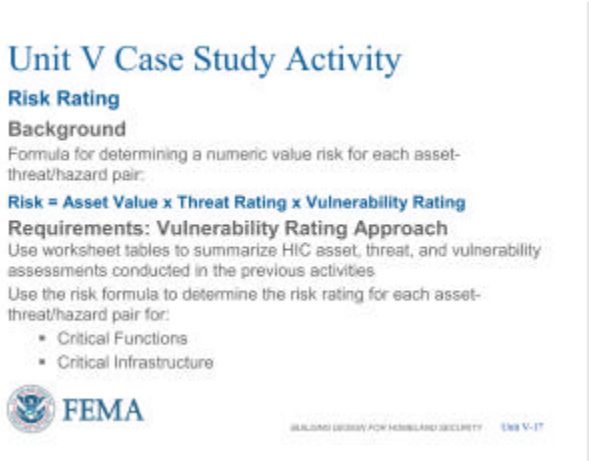
Achieving Building Security

The assessment provides concepts for integrating land use planning, landscape architecture, site planning, and other strategies to mitigate the Design Basis Threats as identified in the risk assessment. Integrating security measures into design and/or maintenance of buildings presents the asset owner with multiple opportunities of achieving a balance among many objectives such as reducing risk; facilitating proper building function; aesthetics and matching architecture; hardening of physical structures beyond required building codes and standards; and maximizing use of non-structural systems.

INSTRUCTOR NOTES	CONTENT/ACTIVITY
VISUAL V-15  	**Process Review** • Calculate the relative risk for each threat against each asset • Identify the high risk areas • Identify Mitigation Options to reduce the risk
VISUAL V-16  	**Summary** • Risk Definition • Critical Function and Critical Infrastructure Matrix • Numerical and color coded risk scale • Identify Mitigation Options

INSTRUCTOR NOTES

VISUAL V-17



Refer participants to the Unit V Case Study activity in the Student Manual.

Members of the instructor staff should be available to answer questions and assist groups as needed.

At the end of 20 minutes, reconvene the class and facilitate group reporting.

CONTENT/ACTIVITY

Student Activity

One approach to conducting a risk assessment is to assemble the results of the asset value assessment, the threat assessment, and the vulnerability assessment, and determine a numeric value of risk for each asset-threat/hazard pair using the following formula:

Risk = Asset Value x Threat Rating x Vulnerability Rating

Activity Requirements

Working in small groups, use the worksheet tables to summarize the HIC asset, threat and vulnerability assessments conducted in the previous three unit activities.

Then use the risk formula to determine the risk rating for each asset-threat/hazard pair identified under Critical Functions and under Critical Infrastructure.

Take 20 minutes to complete this activity. Solutions will be reviewed in plenary group.

Transition

Unit VI will cover Explosive Blast. Unit VII will cover CBR Measures.

UNIT V CASE STUDY ACTIVITY: RISK RATING

One approach to conducting a risk assessment is to assemble the results of the asset value assessment, the threat assessment, and the vulnerability assessment, and determine a numeric value of risk for each asset-threat/hazard pair using the following formula:

Risk = Asset Value x Threat Rating x Vulnerability Rating

Requirement

Use the following tables to summarize the HIC asset, threat, and vulnerability assessments conducted in the previous three unit activities. Then use the formula above to determine the risk rating for each asset-threat/hazard pair identified under Critical Functions and under Critical Infrastructure. Using **Figure 1-13 of FEMA 426**, make a determination of the available risk management options.

Critical Functions

Function	Cyber Attack	Armed Attack	Vehicle Bomb	CBR Attack
1. **Administration Risk Rating**	192	96	192	128
Asset Value	4	4	4	4
Threat Rating	6	3	6	4
Vulnerability Rating	8	8	8	8
2. **Engineering/IT Technicians Risk Rating**	200	120	240	160
Asset Value	5	5	5	5
Threat Rating	5	3	6	4
Vulnerability Rating	8	8	8	8
3. **Loading Dock/ Warehouse Risk Rating**	50	45	240	160
Asset Value	5	5	5	5
Threat Rating	5	3	6	4
Vulnerability Rating	2	3	8	8
4. **Data Center Risk Rating**	810	90	480	320
Asset Value	10	10	10	10
Threat Rating	9	3	6	4
Vulnerability Rating	9	3	8	8

5. **Communications** **Risk Rating**	320	72	384	256
Asset Value	8	8	8	8
Threat Rating	5	3	6	4
Vulnerability Rating	8	3	8	8
6. **Security** **Risk Rating**	105	63	336	224
Asset Value	7	7	7	7
Threat Rating	5	3	6	4
Vulnerability Rating	3	3	8	8
7. **Housekeeping** **Risk Rating**	2	3	48	32
Asset Value	1	1	1	1
Threat Rating	2	3	6	4
Vulnerability Rating	1	1	8	8

Critical Infrastructure

Infrastructure	Cyber Attack	Armed Attack	Vehicle Bomb	CBR Attack
1. **Site** **Risk Rating**	15	120	240	160
Asset Value	5	5	5	5
Threat Rating	1	3	6	4
Vulnerability Rating	3	8	8	8
2. **Architectural** **Risk Rating**	15	120	240	80
Asset Value	5	5	5	5
Threat Rating	1	3	6	4
Vulnerability Rating	3	8	8	4
3. **Structural Systems** **Risk Rating**	15	120	240	60
Asset Value	5	5	5	5
Threat Rating	1	3	6	4
Vulnerability Rating	3	8	8	3
4. **Envelope Systems** **Risk Rating**	15	120	240	60
Asset Value	5	5	5	5
Threat Rating	1	3	6	4
Vulnerability Rating	3	8	8	3

5. **Utility Systems Risk Rating**	75	175	180	60
Asset Value	5	5	5	5
Threat Rating	3	5	6	4
Vulnerability Rating	5	7	6	3
6. **Mechanical Systems Risk Rating**	105	245	336	196
Asset Value	7	7	7	7
Threat Rating	3	5	6	4
Vulnerability Rating	5	7	8	7
7. **Plumbing and Gas Systems Risk Rating**	30	120	240	100
Asset Value	5	5	5	5
Threat Rating	2	3	6	4
Vulnerability Rating	3	8	8	5
8. **Electrical Systems Risk Rating**	105	147	336	140
Asset Value	7	7	7	7
Threat Rating	3	3	6	4
Vulnerability Rating	5	7	8	5
9. **Fire Alarm Systems Risk Rating**	30	45	240	60
Asset Value	5	5	5	5
Threat Rating	2	3	6	4
Vulnerability Rating	3	3	8	3
10. **IT/Communications Systems Risk Rating**	1,000	240	480	240
Asset Value	10	10	10	10
Threat Rating	10	3	6	4
Vulnerability Rating	10	8	8	6